UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

VITOR MEDEIROS

ESTUDO DE VULNERABILIDADES NO USO DA DEEP WEB SOB O PONTO DE VISTA DO USUÁRIO

CRICIÚMA
2018

VITOR MEDEIROS

ESTUDO DE VULNERABILIDADES NO USO DA DEEP WEB SOB O PONTO DE VISTA DO USUÁRIO

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador(a): Professor. Esp. Valter Blauth Junior.

CRICIÚMA

2018

VITOR MEDEIROS

ESTUDO DE VULNERABILIDADES NO USO DA DEEP WEB SOB O PONTO DE VISTA DO USUÁRIO

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Segurança Computacional.

Criciúma, 26 de junho de 2018.

BANCA EXAMINADORA

Prof. Esp. Valter Blauth Junior - Redes de Computadores - UNESC

Prof. Me. Luciano Antunes - Informática na Educação - UNESC

Prof. Me. Paulo João Martins - Sistemas Distribuídos - UNESC

Dedico este trabalho aos meus pais, família e todos os amigos que conheci no decorrer da faculdade e que de alguma forma me ajudaram.

AGRADECIMENTOS

Primeiramente ao meu orientador Valter Blauth Junior por me auxiliar em todo o trabalho desenvolvido e me direcionar com todas as correções necessárias ao projeto.

Segundamente a todos que me ajudaram diretamente e indiretamente fazendo parte da minha formação e que estavam presentes em todas as dificuldades.

“Cada sonho que você deixa pra trás, é um pedaço do seu futuro que deixa de existir.”

Steve Jobs

RESUMO

Esta pesquisa teve como objetivo principal demonstrar de forma prática e teórica as possíveis vulnerabilidades, em que o usuário e seu computador se expõe durante a navegação na *Deep Web* e o vasto problema ao acessar a *Deep Web.* Por se tratar de uma ampla rede de anonimato, em algumas situações podem ocorrer a liberação de diversos itens de segurança do computador, capaz de comprometer a segurança e as informações do usuário. A metodologia aplicada no presente trabalho foi prática e teórica com a utilização de ferramentas, a fim de analisar possíveis portas abertas, registro do sistema operacional Microsoft Windows, processamento e fluxo de dados na rede.

Palavras-chave: Segurança da informação. Deep Web. The Onion Router. Comunicação. Anonimato.

ABSTRACT

The main objective of this research was to demonstrate in a practical and theoretical way the possible vulnerabilities in which the user and his computer are exposed during the navigation in the Deep Web and the vast problem when accessing the Deep Web. Because it is a wide network of anonymity, in some situations the release of various security items from the computer may be able to compromise the security and user information. The methodology applied in the present work was practical and theoretical with the use of tools, in order to analyze possible open ports, registry of the Microsoft Windows operating system, and processing and data flow in the network.

Keywords: Information security. Deep Web. The Onion Router. Communication. Anonymity.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACK	Acknowledge
CE	Cookie de Encontro
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DNS	Domain Name System
DOS	Denial Of Service
DSO	Descritor De Serviço Oculto
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ID	Identificador Descritor
IETF	Internet Engineering Task Force
IP	Internet Protocol
I2P	Invisible Internet Project
NMAP	Network Map Scanner
PI	Pontos de Introdução
P2P	Peer-To-Peer
RFC	Resquest For Comments
RST	Readability Strenght Tone
SDO	Serviço de Diretórios Oculto
SO	Serviços Ocultos
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronize
THD	Tabela Hash Distribuída
TOR	The Onion Router
URL	Uniform Resource Locator
WKP	Well Known Ports
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A *Deep web* conhecida como Internet profunda hospeda sites que por motivos de necessidade de anonimato não são indexados pelos motores de busca da Internet. Sendo assim representam uma porta aberta para atividades ilícitas e cibernéticas.

Os usuários comumente utilizam a chamada *Surface Web* ou “web rasa” onde segundo Pompéo e Seefeldt (2013) a coletânea de páginas são facilmente encontradas por mecanismos de buscas, diferente da *Deep Web* que resume as páginas e por necessidade de anonimato não pertencem a esses provedores, não podendo assim serem listados como resultados. É a definição de indexar as páginas nos mecanismos de buscas que a distinguem como ela será encontrada ou não por esses serviços. Cada página da rede contém padrões que a registram em servidores como Yahoo! e Google.

Para ter acesso a Deep Web existem várias ferramentas, sendo a *The Onion Router* (TOR) uma destas. De acordo com (CIANCAGLINI, 2013) o TOR é uma tecnologia gratuita e pode ser obtido e utilizado por qualquer usuário e para acesso a Deep Web através da Internet. Esta rede permite comunicações anônimas através de nódulos voluntários que são responsáveis por traçar uma rota de pedidos criptografados para que o trânsito de dados possa passar despercebido por ferramentas de monitoramento.

Sendo assim, durante a sua instalação e funcionamento podem ocorrer a liberação de diversos itens de segurança tais como portas de acesso, controle da máquina, processamento e outros. Com o intuito de aprofundar os conhecimentos sobre a *Deep Web* utilizando esta ferramenta, o presente estudo pretende demonstrar a vulnerabilidade da máquina e do usuário através de experimento prático e teórico desde a instalação até a navegação propriamente dita.

1.1 OBJETIVO GERAL

Demonstrar de forma prática as vulnerabilidades do usuário durante a navegação na Deep Web.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos consistem em:

a) analisar os efeitos da instalação e uso destas ferramentas do ponto de vista do usuário;
b) analisar as alterações do ponto de vista do Sistema Operacional;
c) sugerir ações de prevenção e uso consciente para acesso a Deep Web.

1.3 JUSTIFICATIVA

Após pesquisar artigos relacionado a Deep Web surgiu o interesse em analisar as possíveis vulnerabilidades de segurança do computador e de seus usuários, pois nesta rede oculta todas as informações estão baseadas em fóruns e blogs na tentativa de manter o anonimato para dificultar o rastreamento por parte das autoridades. De acordo com Pompéo e Seefeldt (2013) por não haver uma lei específica que regulamente a Internet como um todo é grande a facilidade do armazenamento de dados ilegais e diversas práticas criminosas.

Dentre as ferramentas de acesso à rede *Deep Web* o *The Onion Router* é o navegador mais utilizado, tendo como característica gratuidade, código aberto e fácil acesso uma vez instalado no computador ela esconde a identidade do usuário na internet, impedindo assim identificar as tarefas e a identidade do usuário durante a sua utilização. De acordo com Bergman (2001), a garantia do anonimato se dá ao rotear dados por redes distribuídas. Estas redes distribuídas são servidores, que são gerenciados por voluntários do mundo todo. Sendo assim quando solicitado a acessar um dado é transcorrido por vários servidores distribuídos até chegar ao destino final, ao usar o TOR, o rastreamento de ambos se tornam inviáveis.

Sendo assim, foi desenvolvido este trabalho para demonstrar possíveis vulnerabilidades ao acessar a Deep Web com a ferramenta TOR. Para isto – foram efetuadas efetuado análises e o monitoramento da instalação.

1.4 ESTRUTURA DO TRABALHO

Este trabalho de pesquisa é constituído por sete capítulos, sendo que o primeiro capítulo aborda uma introdução sobre o tema da pesquisa, e sua estrutura é formada pela introdução, objetivo geral e seus objetivos específicos, e da justificativa para o qual o projeto será desenvolvido.

No segundo capítulo faz-se citação sobre a passagem pela história da Internet, o que são os protocolos e Internet de superfície.

No terceiro capítulo faz-se a menção da Deep Web, histórias e páginas não indexadas, o funcionamento do software TOR, em citação de outras ferramentas de acesso anônimo a páginas não indexadas da Internet, nas quais, serão feitos as análises desde a instalação até o acesso propriamente dito. Contendo várias ilustrações explicativas.

No quarto capitulo é abordado sobre a segurança da informação, os padrões de segurança, funcionamento das políticas de segurança e as criptografias.

O capítulo cinco trata dos trabalhos correlatos a este projeto de pesquisa.

O capítulo seis, é definido a metodologia a ser utilizada para o desenvolvimento.

O capítulo sete, é demonstrado toda apresentação e análise dos dados obtido através dos testes realizado com as ferramentas propostas pela metodologia.

Para finalizar, o capitulo 8 e descrito a conclusão de todo o projeto proposto.

2 INTERNET

A Internet é formada por um movimento constante de informações ilimitadas, é um meio global de comunicação em tempo real, ou seja, todos podem manifesta-se e tem a liberdade de expressão.

Basta apenas ter um dispositivo eletrônico conectado à Internet para poder informar e informar-se.

A sociedade deixa de estar conectada localmente e passa a estar conectada globalmente, com acesso a informação do mundo todo (NASCIMENTO, 2009).

A era da informação e o mundo digital faz totalmente parte da realidade atual, com o fácil acesso à internet surge a cibercultura, que é um conjunto de técnicas, práticas, atitudes, modos de pensamentos e valores que se desenvolvem juntamente com o ciberespaço, que é o novo meio de comunicação que surgiu da interconexão mundial dos computadores, o termo especifica não apenas a infraestrutura material da comunicação digital mas também o universo oceânico de informações que ele abrange, assim como as sociedades que a utilizam e alimentam este universo (LÉVY, 2003).

Com o avanço tecnológico no presente século XXI, segundo Castells e Cardoso (2005) pessoas, empresas e instituições utilizam e constroem por si mesmas e para si, um novo meio de comunicação através de diferentes ferramentas, smartphones, computadores, sites, todos com o propósito da comunicação, informação, entretenimento, relacionamento, comércio, mídia, política entre outros.

Cada usuário conectado à Internet somente poderá navegar após possuir uma identidade “endereço eletrônico” e passar por protocolos, normas e regras. Com esta identidade o indivíduo consegue facilmente acessar e utilizar todas as ferramentas possíveis e disponíveis. Há dois tipos de internet a *Deep Web* “internet profunda” e a *Surface web* “internet de superfície”, a *Surface web* tem leis aplicáveis, enquanto a *Deep Web* não tem a ser visto adiante.

2.1 PROTOCOLOS

Os primeiros especialistas em desenvolvimento trabalharam rigorosamente para efetuar a ampliação do alcance das redes, com o intuito de compartilhar conhecimentos e melhorar a acessibilidade das tecnologias desde o surgimento. Eles foram os primeiros hackers, conhecidos ainda hoje por uma forma ofensiva, sendo tratados de forma errada, pois eles tiveram um papel imprescindível para a cultura da Internet. Eles desenvolveram os protocolos da rede que sustentavam a liberdade de comunicação assim formando a Internet independente de força política, pública, privada ou corporativa (ARAUJO,2013).

Estes protocolos em tempos anteriores havia um grande desafio para expansão e globalização da Internet. Foi o momento da discussão sobre padronização. A Europa defendia o padrão x.25 onde acreditavam que o controle deveria ser feito através dos provedores da rede pública. Porém com este protocolo não era possível comunicar com o protocolo Arpanet TCP/IP, que era flexível para integrar todos os dispositivos na rede. Sendo assim, após uma longa discussão entre governos, operadoras de telecomunicações e fabricantes de computadores prevaleceu o TCP/IP. As organizações sem fins lucrativos como a Internet *Society* e a Internet *Engineering Task Force* (IETF) ficaram responsáveis pelo cuidado do protocolo TCP/IP e trabalham publicando *Request For Comments* (RFC), que são os documentos que detalham padrões utilizados na rede (CASTELLS, 2003).

Os usuários geralmente pensam como pode-se comprar em um site da Web, dando informações pessoais e sentir-se remotamente seguros. Certamente está enviando dados de identificação individual, sem guia ou guarda, na gigantesca extensão do ciberespaço. Aguardar que suas informações cheguem ao lugar certo, com segurança, parece colocar a fé em como um milagre. O segredo está em um protocolo uma boa criptografia conhecido como protocolo HTTP/HTTPS (CASTELLS, 2003).

Estes protocolos ambos focados em transferência de hipertexto através de hiperlinks, onde normalmente inicia quando um usuário clica em cima de um ícone em uma página *HyperText Markup Language(HTML)* que é um padrão de representação onde especifica a sintaxe para a página web, ou seja, o texto âncora. O HTML permite que um programador especifique na página web um gráfico, vídeo e áudio por exemplo. Este protocolo deveria ser chamado de hipermídia em vez de

hipertexto, pois permite que uma imagem contenha um link para outra página (GALLOWAY, 2004).

O *HyperText Transfer Protocol* (HTTP) é um protocolo da camada de aplicação, o que significa que ele se concentra em como a informação é apresentada ao usuário do computador, mas não se preocupa com a forma de como os dados saem do ponto A ao ponto B. Ou seja, significa que ele não tenta lembrar nada sobre a sessão anterior da Web ele simplesmente leva a informação, porque há menos dados para enviar, e isso lhe dá mais velocidade. O protocolo HTTP opera na Porta 80 do Protocolo de Controle de Transmissão (TCP) por padrão, podendo ser alterada, o que significa que seu computador deve enviar e receber dados através desta porta para usar o HTTP (SILVEIRA, 2009).

De acordo com Silveira (2009) ele é usado para informações de hipermídia, no qual é reunida diversas mídias em um ambiente computacional, ou seja, ele é a base para a comunicação de dados da *World Wide Web* (WWW). Com HTTP, é possível abrir o navegador e interagir com os dados. O trabalho do HTTP é apresentar esses dados, e os navegadores são o meio de fazê-lo. O protocolo HTTP trabalha diferentes design dependendo do navegador, proporciona velocidade porém sem a segurança.

Preocupados com isso surgiu um novo protocolo, conhecido como *Secure HyperText Transfer Protocol* (HTTPS). A principal distinção é que ele usa a porta TCP 443 por padrão, então HTTP e HTTPS são duas comunicações separadas. O HTTPS funciona em conjunto com outro protocolo, *Secure Sockets Layer* (SSL), para transportar dados com segurança. Ele não deixa nada para trás, fazendo com que a navegação seja mais lenta e segura. HTTP e HTTPS não se importam com a forma como os dados chegam ao seu destino. Em contraste, o SSL não se importa com o aspecto dos dados. O HTTPS é seguro porque usa SSL para mover dados. HTTPS com o SSL leva os dados de forma segura do ponto A para o ponto B e criptografa, ele faz isso através de um algoritmo matemático, e este algoritmo é tão complexo que é improvável que seja quebrado (DOTSON, 2007).

Para facilitar o acesso dos usuários foi criado o protocolo *Domain Name System* (DNS) que fornece um objetivo, é mapear nomes simbólicos legíveis aos seres humanos para endereços de computadores, através dos navegadores, softwares, e-mail e a maioria dos aplicativos da Internet usam DNS. Eles são compostos de muitos servidores para este serviço. São dispostos a uma hierarquia e

cada um deles conhece a localização de todos na hierarquia, usando um cache por exemplo para manter a eficiência. Este DNS é usado na *Surface Web* ou Internet de superfície a ser visto (COMER, 2016).

2.2 INTERNET DE SUPERFÍCIE

A Internet de superfície também conhecida como *Surface web* é a qual o usuário tem contato diariamente com um dispositivo conectado na Internet. A *World Wide Web* (protocolo HTTP) é um subconjunto de conteúdo da Internet onde a transmissão de dados ocorre através de servidores e são exibidos em hipertextos, conhecidos como links, ao clicar com o mouse em cima direciona de uma página para outra, e também os robôs conhecidos como “aranhas”, são programas inteligentes cujo trabalho é a busca, indexação e catalogação de informações. O problema ocorre quando as informações necessárias estão em uma página que não possui links, nesse caso, a única maneira de registrar esta página em um mecanismo de busca, é o autor incluir manualmente preenchendo um formulário, caso contrário, esta web será invisível para todos os usuários da Internet que não conheçam o URL ou o endereço específico (POMPÉO E SEEFELDT, 2013).

A maioria dos usuários conhecem apenas o conteúdo que é apresentado através de navegadores, onde digitam palavras chaves em mecanismos de busca conhecidos como Google, Yahoo!, Bing e outros, estas informações estão em páginas da web, onde todos os sites cuja informação pode ser indexada pelos robôs dos motores de busca convencionais e recuperada quase na sua totalidade por meio de uma consulta às suas formas de busca, ou seja, todas as páginas que estão indexadas é porque cumprem as regras estabelecidas, os índices irão indicar o quão relevante ela é, por exemplo em uma pesquisa, uma página de produtos automotivos bem sucedida e que contém todas especificações dos produtos e todo o conteúdo explicativo, será mais acessada, por fim ela ficará no topo das pesquisas e este site se tornará conhecido por todos e terá um sucesso em vendas (PALACIOS, 2014).

Os motores de busca obtêm suas listas de duas maneiras: os autores podem enviar suas próprias páginas da Web, ou os mecanismos de pesquisa conhecido como "aranha", seguindo um link de hipertexto para outro, os rastreadores que são responsáveis por localizarem e registrarem todos os links de

hipertexto que cada página contém, como se fossem ondulações que se propagam em uma lagoa onde podem ampliar mais e mais longe do seu ponto de partida (PALACIOS, 2014).

A superfície da Web contém aproximadamente 2,5 bilhões de documentos, crescendo a uma taxa de 7,5 milhões de documentos por dia. Os maiores motores de busca fizerem um trabalho impressionante ao ampliar seu alcance, embora o próprio crescimento da Web excedesse a capacidade de rastreamento dos motores de busca, hoje há diversos motores de busca sendo os maiores em termos de documentos indexados internamente é o Google com 1,35 bilhão de documentos (500 milhões disponíveis para a maioria das pesquisas) e com 575 milhões de documentos onde em segundo lugar o *Northern Light* com 327 milhões de documentos.

As críticas logo vieram e foram discutidas contra os motores de busca com rastreamentos de hipertextos indiscriminados, ou seja, porque eles fornecem muitos resultados, pesquisa como palavra-chave "Web", por exemplo, com o *Northern Light*, cerca de 47 milhões de visitas. Além disso, novos documentos são encontrados a partir de links dentro de outros documentos, os documentos citados são mais prováveis de serem indexados do que os novos documentos, até oito vezes mais prováveis (BERGMAN, 2001).

Para superar essas limitações, a geração mais recente de mecanismos de busca (notadamente o Google) substituiu a abordagem de ligação aleatória com rastreamento direto e indexação com base na "popularidade" das páginas. Nessa abordagem, os documentos mais frequentemente referenciados que outros documentos têm prioridade tanto para o rastreamento quanto para a apresentação dos resultados. Esta abordagem fornece resultados superiores quando as consultas simples são emitidas, mas ainda a tendência de ignorar documentos com poucos links (BERGMAN, 2001).

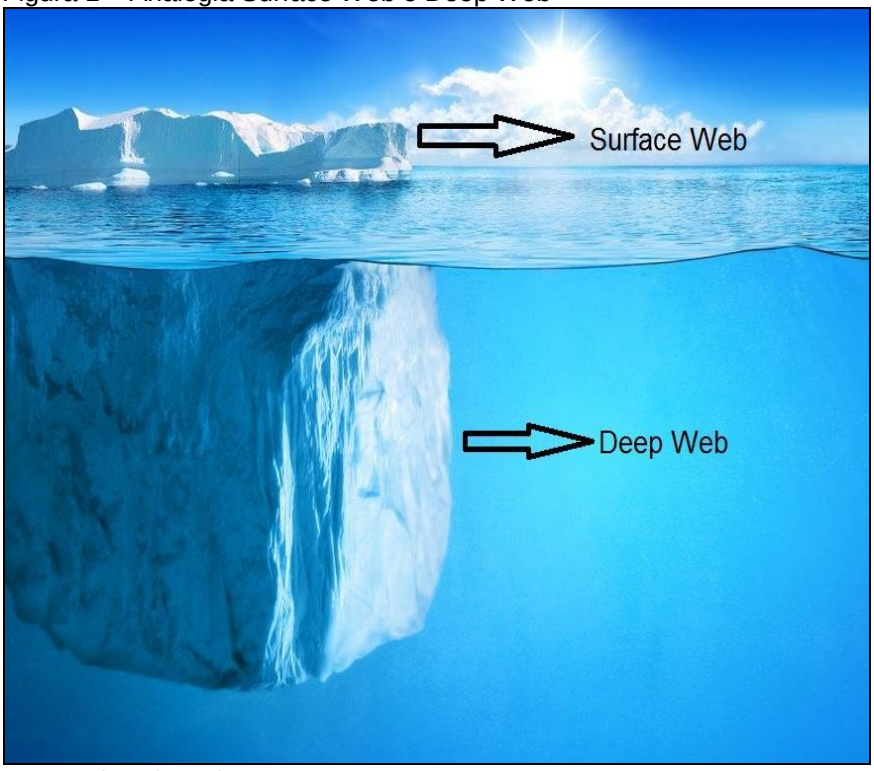
Uma vez que um mecanismo de pesquisa precisa atualizar literalmente milhões de páginas da Web existentes, a fração de seus resultados sofre. Numerosos comentadores notaram o aumento do atraso na publicação e registro de novas informações nos motores de busca convencionais, além disso, voltando para a premissa de como um mecanismo de pesquisa obtém suas listas em primeiro lugar, seja ajustado para popularidade ou não, ou seja, sem uma ligação de outro documento da web, a página nunca será descoberta. Mas a principal falha nos

motores de busca é que eles dependem dos links da Web para identificar o que está na Web (BERGMAN, 2001).

Atualmente, a possibilidade de indexar arquivos não-textuais, como imagens, áudio, vídeo, arquivos PDF, arquivos compactados ou programas executáveis tornou-se um desafio para motores de busca mais convencionais, tecnicamente, a maioria desses formatos pode ser indexada, mas muitos pesquisadores optam por não fazê-lo porque esses formatos são mais difíceis de arquivar e organizar, exigindo mais recursos de servidor e um custo econômico mais elevado (BERGMAN, 2001).

Oitenta e cinco por cento dos usuários da Web usam mecanismos de pesquisa para encontrar a informação necessária, é uma porcentagem tão alta onde a incapacidade de encontrar a informação desejada, como uma das suas maiores frustrações. Mas nem tudo que se pesquisa está nos mecanismos de busca, ou seja, ao pensar que o conteúdo pesquisado não existe, por exemplo no Google, pode estar errado, basta apenas pesquisar profundamente. Fazendo uma analogia, a *Surface web* é apenas a ponta de um iceberg e o montante abaixo é a *Deep Web* (PISAREWICZ, 2013).

Figura 1 – Analogia Surface Web e Deep Web



Fonte: Lima (2017).

A Figura 1 demonstra a analogia da quantidade de informações e dados comparando a *Surface Web* e *Deep Web*. Pode-se observar nesta analogia que a *Surface web* ou web rasa tem apenas um terço da quantidade de dados se comparado com a *Deep Web* ou web oculta, porém a grande maioria dos usuários desconhecem a quantidade de informações que a *Deep Web* abrange ou desconhecem de como utilizar e acessar a ser visto adiante (PISAREWICZ, 2013).

3 DEEP WEB

De acordo com Pompéo e Seefeldt, “a expressão *Deep Web* foi criada por Michael K. Bergman, fundador do programa Bright Planet, software especializado em coletar, classificar e procurar conteúdo nessa esfera da web.” (POMPÉO; SEEFELDT, 2013, p.440).

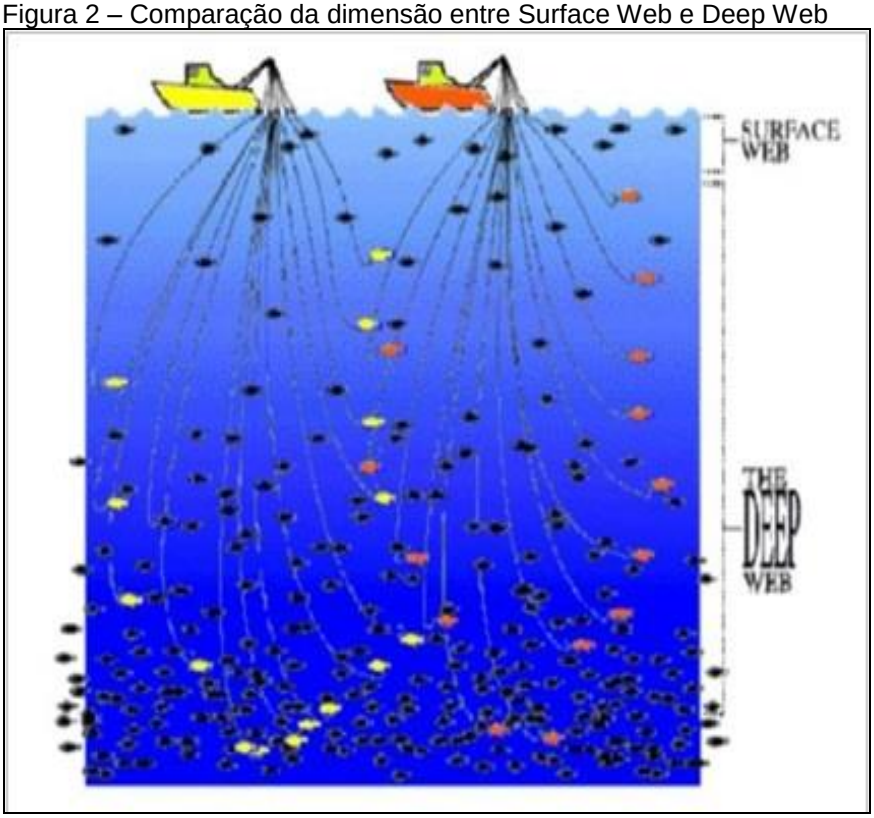
A *Deep Web* conhecida como “web oculta”, preza o anonimato de seus usuários representando assim uma porta aberta para a realização de atividades ilícitas como: drogas, prostituição, pornografia, pedofilia, contrabando de mercadorias, materiais radioativos, tráfico de órgãos humanos, organização de jogos de azar, conter documentos do governo, sequestros dentre outros cibercrimes. Ainda não há tecnologia que possa tornar os seres humanos físicos invisíveis, mas é possível ser anônimo e, de certa forma, "invisível", na Internet, o *software The Onion Router* e navegando na *web* que é conhecido como a Internet profunda (BERGMAN, 2001).

Toda informação pesquisada mais profundamente na *Deep Web* é possível encontrar, não havendo decepções. Ao acessar esta profundeza deve-se tomar muito cuidado, por ser anônimo e conter páginas que por algum motivo não respeitam as regras solicitadas. Elas se tornam páginas de web não indexadas por provedores de busca, isto é, em uma requisição de informação no Google por exemplo, ele não irá conseguir obter a informação a respeito do hiperlink da página *Deep Web* e não conseguirá acessá-la (BERGMAN, 2001).

Diversas analogias são feitas para representar a dimensão da *Deep Web*, uma delas é a analogia feita com o mar, em que se faz referência a uma pessoa que está nadando, consegue visualizar apenas a superfície da água, mas que, com os devidos equipamentos de mergulho, pode emergir e descobrir um mundo que antes era invisível. O mesmo acontece na web com poucos recursos, apenas com navegadores os usuários acessam a superfície, porém sem os instrumentos precisos de maneira alguma conseguirá chegar à profundeza.

Por fim, existe outra relação que faz citação a um grupo de pescadores em um navio em alto mar. Quando jogam uma rede de pesca na área superficial de um mar, a probabilidade de pescarem peixes é muito pequena se comparada com a mesma rede jogada em maior profundidade. Sendo assim, quanto mais profundo for o alcance, maior o retorno que será obtido a ser ilustrado na figura 2.

Figura 2 – Comparação da dimensão entre Surface Web e Deep Web



Fonte: Bergman (2012).

A *Deep Web* é conhecida como Internet profunda e anônima, por vasto conteúdos ilícitos e de cibercrimes. Comumente utilizada por pessoas “usuários” mal intencionados. Sendo assim, o potencial de informações na Deep Web não se dá apenas por conteúdos ilícitos ou cibercrimes. Como afirmam Martins e Silva (2013) fica a escolha do usuário como será feito a escolha dos assuntos no qual se propõe encontrar nesta profundidade da rede.

O usuário está focado em encontrar documentos, informações científicas, livros e fatos não publicados por terem uma alta censura que possuem no acesso da *Surface Web*, seja porque determinados arquivos ou informações que estão sendo buscado, encontram-se mais ao final da indexação dos mecanismos de busca convencionais, ou seja, porque tal conteúdo está pouco difundido na rede (BERGMAN, 2001).

Ele terá uma abrangência maior e uma grande chance de conseguir encontrar os conteúdos e arquivos na Internet profunda de uma forma ágil. Essa agilidade se interpreta em qualidade, pois, conforme dito anteriormente, ele conseguirá encontrar o que se propôs a buscar. Cabe destacar que por não haver

a necessidade de se respeitar uma lei em vigor no que diz respeito à este espaço cibernético, diversos conteúdos e arquivos estão disponíveis integralmente, basta apenas utilizar os recursos corretos.

Segundo Martins e Silva (2013) nos mostram as possibilidades de navegar na Deep Web e encontrar conteúdo legal. Os autores também exemplificam de que forma buscar os conteúdos:

> O *Infomine* é um mecanismo de busca específico para conteúdo de bibliotecas universitárias norte-americanas, entre elas a Universidade da California; o *Intute* permite acesso ao conteúdo de todas as universidades da Inglaterra; o *Complete Planet* dá acesso a assuntos diversos, como militares, comidas ou meteorologia para agricultores; o *IncyWincy* possui busca por imagens; o *DeepWebTech*, permite acesso a temas como medicina, negócios e ciências; o *Scirus* é direcionado para assuntos científicos, como jornais, homepages de cientistas, materiais didáticos e patentes; o *TechXtra* é direcionado para a área de exatas, como matemática, engenharia e computação. [...] Há aqueles que usam a Web Invisível para armazenar informações que precisam gerar tráfego, como por exemplo, resultados parciais de pesquisas, e o simples armazenamento de bases de dados organizacionais que não estão sendo utilizadas no momento. (MARTINS; SILVA, 2013, p.4).

A *Deep Web* é pelo menos 400-500 vezes o tamanho da *Surface Web*. Está crescendo continuamente, e isso significa que novas fontes da Deep Web também estão crescendo. Para acessar esta Internet profunda utiliza-se diferentes softwares que deixa o usuário anônimo na Internet, o mais conhecido *The Onion Router* (TOR) (PEDERSON, 2013).

3.1 THE ONION ROUTER

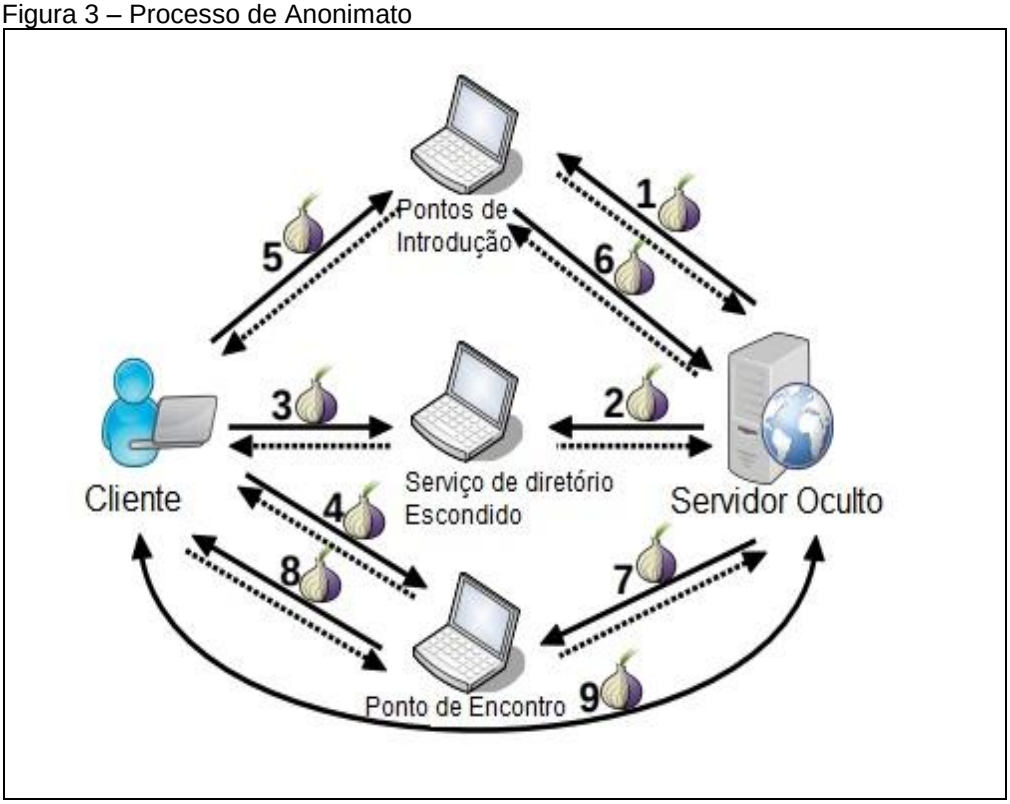
Na era da vigilância em massa, a privacidade e segurança na Internet tornou-se uma preocupação. Várias abordagens foram propostas para comunicação anônima, mas apenas algumas delas chegaram até a implantação generalizada. Tor é o software de baixa latência mais popular na rede. O seu desenvolvimento inicial foi para o Laboratório de Pesquisa Naval Americano, visando assegurar a comunicação governamental. Hoje, ele é usado diariamente por “pessoas normais” sendo governos, usuários curiosos, militares, policiais, jornalistas, entre outros. Permitem aos usuários, em particular aqueles que vivem em regimes opressivos, por exemplo, ativistas dos direitos humanos e denunciantes, ignorar a censura e exercer

liberdade de discurso por publicar e oferecer acesso ao conteúdo sem ser perseguidos, presos ou forçados a desligar seus serviços (CIANCAGLINI, 2013).

Ele visa esconder o endereço IP do usuário enquanto comunica-se na Internet. Sua utilização é ampla entre os setores e as classes sociais. A troca de tráfego entre o remetente e o destinatário é criptografado e anônimo. O cliente, ao iniciar uma conexão, executa um "*onion proxy*" que é criar um túnel virtual, chamado de circuito. Neste túnel o TOR torna o usuário invisível por entre os outros usuários que utilizam a rede, ou seja, a quantidade de pessoas que o utilizam é, na verdade, que o torna tão seguro. Quanto maior for a base de pessoas e distribuída esta base globalmente, maior o anonimato será protegido (TOR PROJECT, 2017).

O TOR é utilizado para proteger os usuários das ferramentas de vigilâncias da Internet ou chamadas de "análise de tráfego", ela é usada para espionar quem está falando com quem, quanto tempo levou ou até mesmo o que foi conversado, mesmo sendo uma conexão criptografada. Saber a origem e destino do tráfego da Internet permite que outras pessoas possam saber dos seus interesses ou até comportamentos. Um usuário, por exemplo, que está em viagem e acessa informações do seu país de origem e cria um site de comércio eletrônico, onde ele discrimina os valores dos produtos, provocando assim a queda de vendas dos comerciantes. Pode acarretar diversos problemas como a segurança física, revelando quem e onde está. Com o TOR isto não é possível, pois o usuário se torna anônimo (SILVEIRA, 2009).

Figura 3 – Processo de Anonimato



Fonte: Tor Project (2017).

As funcionalidades dos serviços ocultos (SO) do TOR. A Figura 3 ilustra as etapas para configurar um SO através do TOR e estabelecer uma conexão com ele. O operador do servidor executa na ordem um *onion proxy* para ligar o servidor via TOR. Depois o servidor *union proxy* seleciona três ORs, conhecidos como pontos de introdução (PI) e cria um circuito separado para cada um deles. (Etapa 1). O servidor informa aos PIs os dados e a chave do serviço associando o endereço.

O uso das chaves de serviço em um PI previne o rastreamento das atividades através do SO, que por algum motivo não são capazes de ser reconhecido a qual serviço elas estão servindo. Em seguida, o servidor gera um mecanismo de informação conhecido como descritor de serviço oculto (DSO). Este descritor contém a chave pública que está associada ao seu SO e a uma lista dos PIs com as correspondentes chaves de serviço. Para fazer uma publicação, o descritor anônimo é chamado como serviço de diretórios oculto (SDO), serve para anunciar anonimamente o seu serviço no TOR, (ETAPA 2).

O DSO fornece uma porta aberta para armazenar e servir em um tempo de atividade de pelo menos 96 horas. Com base no identificador do descritor (ID), o SO determina um DSO que será responsável por manter seu descritor. No TOR, os DSOs são representados na forma de uma tabela *hash* distribuída (THD) onde cada

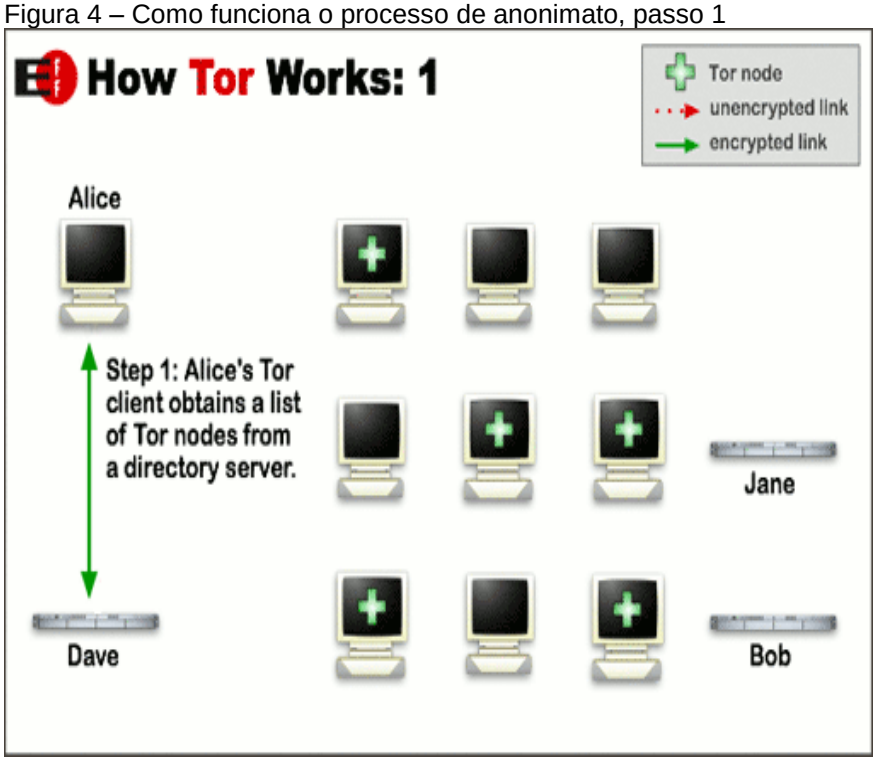
descritor de SO é identificado por sua impressão digital. Os três primeiros descritores de SO consecutivos, cujas impressões digitais são maiores do que a ID do descritor, são selecionados para armazenar o DSO. Para acessar um SO, o cliente necessita obter seu endereço.

O endereço do SO, também chamado de *onion address*, está na forma de x.onion onde x denota os primeiros 80 bits do *hash* da chave pública do SO. O cliente calcula a ID do descritor correspondente para recuperar uma lista de DSO responsável. Para entender os endereços dos PIs, o trajeto do SO e as chaves de serviço correspondentes associadas a estes PIs. (ETAPA 3). Antes de se conectar a um PI, o cliente cria um circuito para um OR selecionado aleatoriamente, chamado ponto de encontro (PE), (ETAPA 4). Envia um valor arbitrário do cookie de encontro (CE) para esse OR. Em seguida, o cliente cria um novo circuito para um dos PI do SO para informar o SO sobre a ID do PE selecionado e o CE, (ETAPA 5).

O PI encaminha esta informação para o SO (ETAPA 6). Se o SO aceitar o pedido do cliente, ele constrói um novo circuito no PE (ETAPA 7). Se o PE reconhecer o CE enviado pelo SO, ele informa o cliente que a conexão com o SO foi estabelecida (ETAPA 8). Subsequentemente, o PE começa a transmitir de forma transparente os pacotes criptografados entre o cliente e o SO (ETAPA 9). Além dos SOs publicamente acessíveis, o servidor pode ser configurado para permitir apenas clientes autorizados para acessar seu serviço. O TOR específica a implementação de dois protocolos para configurar a autorização do cliente.

Ao invés de escolher entre uma rota direta origem e destino, os pacotes de dados na rede TOR seguem um túnel aleatório através de diversos servidores distribuídos em que nenhum “observador”, mês que esteja em qualquer ponto, não conseguirá saber de onde vêm os dados e nem para onde vão. É por isso que a navegação através do software TOR se dá de maneira mais lenta comparado a um navegador comum, tendo uma leve impressão de estar “amarrado”, pois o usuário comum está acostumado com o Internet Explorer, Mozilla Firefox ou Google Chrome por exemplo. Nesta Figura a seguir o funcionamento das conexões.

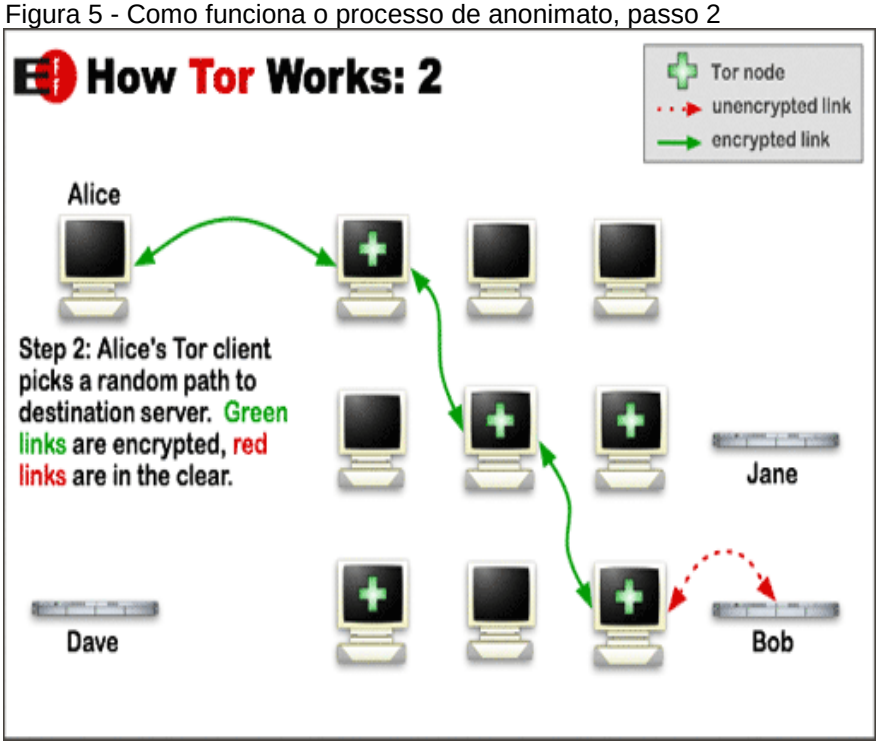
Figura 4 – Como funciona o processo de anonimato, passo 1



Fonte: Tor Project (2017).

Nesta figura 4 a cliente Alice, obtém uma lista de nós TOR de um servidor de diretório, ponto a ponto. O link cor verde representa que onde ela está é criptografado, não havendo nenhum perigo de identificação e análise de tráfego. Neste caso se ela fosse uma jornalista querendo publicar globalmente uma matéria confidencial, perigosa e privada sem expor sua identidade, ou pesquisando uma matéria que por algum motivo está bloqueada na *Surface Web*. Ela teria liberdade, privacidade e segurança na publicação ou na troca de informação e conhecimento.

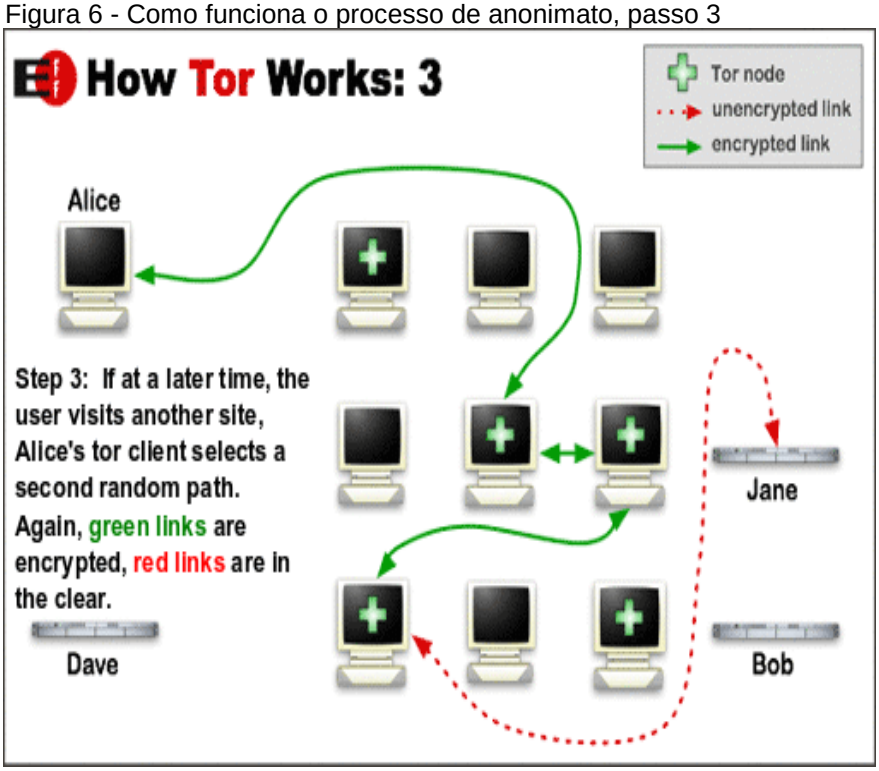
Figura 5 - Como funciona o processo de anonimato, passo 2



Fonte: Tor Project (2017).

A cliente do TOR Alice, escolhe um caminho aleatório para o servidor de destino. Os links verdes são criptografados, os links vermelhos não estão criptografados. Ou seja, caso a Alice precise acessar uma matéria jornalística que está em um servidor oculto Bob, todo o caminho será anônimo. Neste caso ao passar por todos esses nós através de túnel, na análise de tráfego irá saber onde esta matéria se encontra porém não conseguirá saber quem o acessou, graças ao software TOR com sua tecnologia do anonimato. Se, posteriormente, ela visitar outro site, ao selecionar um segundo caminho aleatório. Como a seguir neste outra ilustração. Novamente, os links verdes são criptografados e os links vermelhos não estarão criptografados.

Figura 6 - Como funciona o processo de anonimato, passo 3



Fonte: Tor Project (2017).

Por não ser o único software de anonimato poderá ser estudado e obter informações futuras.

3.2 FREENET

O Freenet é uma rede *peer-to-peer* (P2P) ou seja uma conexão ponto a ponto onde cada ponto pode ser tanto cliente como servidor, nesta conexão não existe um servidor central, ela foi projetada para permitir a distribuição de informações através da Internet de forma eficiente e anônima. O primeiro lançamento da Freenet na Internet ocorreu em abril do ano 2000. Neste ano foi efetuado nove lançamentos de diferentes versões. Desde então, o software Freenet foi baixado mais de 2.000.000 vezes da Internet. Isso mostra o interesse do público neste software (CIANCAGLINI, 2013).

Os objetivos gerais da Freenet conforme definidos, a rede não deve ter controle ou administração centralizada ela contém um algoritmo tão complexo que é praticamente impossível remover de forma forçada uma informação da rede. Por ser P2P tanto os autores quanto os leitores de informações devem permanecer anônimos se assim o desejarem. Toda a informação é distribuída para toda a rede

de forma que seja difícil para determinar onde as informações estão sendo armazenadas, a disponibilidade das informações deve aumentar em proporção da demanda. A informação se move de partes da Internet onde está em baixa demanda para áreas onde a demanda é maior.

Os documentos são armazenados ou inseridos na rede com um endereço ou chave associada, Ian Clarke, Oskar Sandberg, Matthew Toseland, Vilhelm Verendel relatam que esta chave consiste em uma *string* binária. É usada tanto para decidir na rede onde o documento será armazenado, autenticar o documento quando ele é transferido. Uma pessoa que deseja acessar o documento envia uma consulta de recuperação ou solicitação, que executa uma pesquisa conhecida como *backtracking* que é um algoritmo que utiliza um refinamento de força bruta onde diversas soluções podem ser eliminadas sem se quer examinadas anteriormente. Quando a solicitação encontrar um nó contendo uma cópia do documento, todo o documento é retornado através do caminho de pesquisa (FREENET PROJECT, 2017).

Os nós Freenet não garantem a persistência de documentos, os nós armazenam de maneira muito agressiva, então é necessário um sistema para remover documentos do cache. Assim podendo ser vista como uma grande rede de hosts e proxy de cache. Sem nenhuma fonte para retornar se o documento não estiver no cache. Na prática, verifica-se que o sistema é relativamente bom na manutenção de dados quando uma quantidade suficiente de armazenamento está disponível.

As funcionalidades da Freenet têm ampliado além da simples publicação de conteúdo: Freesites, sites completos hospedado em Freenet. Ele oferece a possibilidade de armazenar e recuperar grandes quantidades de informação, um sistema de mensagens instantâneas e um sistema de e-mail foram construídas também sobre o Freenet. Todos esses componentes usam a mesma aplicação independente de algoritmos e protocolos para armazenar, encontrar e recuperar conteúdo, que serão discutidos. Primeiro, eles explicam que os usuários e os arquivos são identificado em Freenet. Posteriormente, discutem como os dados são armazenados e recuperados, antes de detalhar como a topologia é criada (CLARKE, 1999).

Na Freenet, usuários e arquivos são identificados e verificados usando chaves criptográficas. As chaves públicas e privadas de um usuário são criadas

após a inicialização de seu nó e costumava assinar arquivos publicados. Além disso, cada nó tem uma localização, isto é, uma chave para o qual os arquivos são mapeados. Em analogia com o identificador de um *peer* em uma tabela de *hash* distribuída, os nós do Freenet são responsáveis pelo armazenamento de arquivos cuja a chave está próxima da sua localização.

Este projeto atualmente recebe ajuda de desenvolvedores globalmente conectados e experientes, eles recebem doações de diversas pessoas "colaboradores" para manter o projeto, diversas versões são publicadas anualmente, melhorando o mecanismo de anonimato P2P.

3.3 INVISIBLE INTERNET PROJECT

I2P é uma rede de anonimato de baixa latência orientada para mensagens baseada em ponto a ponto que oferece aos seus usuários interagir dentro da rede e um nível de prevenção de análise de tráfego. Assim formando uma rede de comunicação totalmente anônima entre duas partes ocultando a identidade do usuário. Ele foi apresentado pela primeira vez no ano de 2003, tendo suas raízes no *Invisible Internet Project* (IIP), contendo ampla escala de aplicações que estão disponíveis dentro da rede I2P, por exemplo, *web-hosting* anônimo, navegação na web, compartilhamento de arquivos, torrentes, e-mail e muito mais (CONRAD e SHIRAZI, 2014).

Ele é um sistema baseado em mensagens, sendo assim, um sistema totalmente distribuído que não depende de servidores de diretório centralizados para manter rastreamento dos nós participantes e desempenho da rede. Tecnicamente, a rede I2P é uma aplicação múltipla estrutura Java que foi projetada para providenciar informações anônimas P2P *networking*. Cada usuário que contem a rede aberta está com o chamado I2P roteador ativo, a parte central do *software* I2P. Todas as mensagens são retransmitidas através de túneis criados por cada roteador I2P usando outros túneis I2P.

Os túneis só podem ser usados em uma direção, o tráfego de saída e de entrada precisam ser construídos. A antologia dos pares é feita através de um algoritmo de seleção baseado em camada, que está em execução por cada roteador I2P. Após se concretizar a entrada e saída, os clientes dos túneis podem promulgar suas informações de influência em um banco de dados global, chamado netDB. O

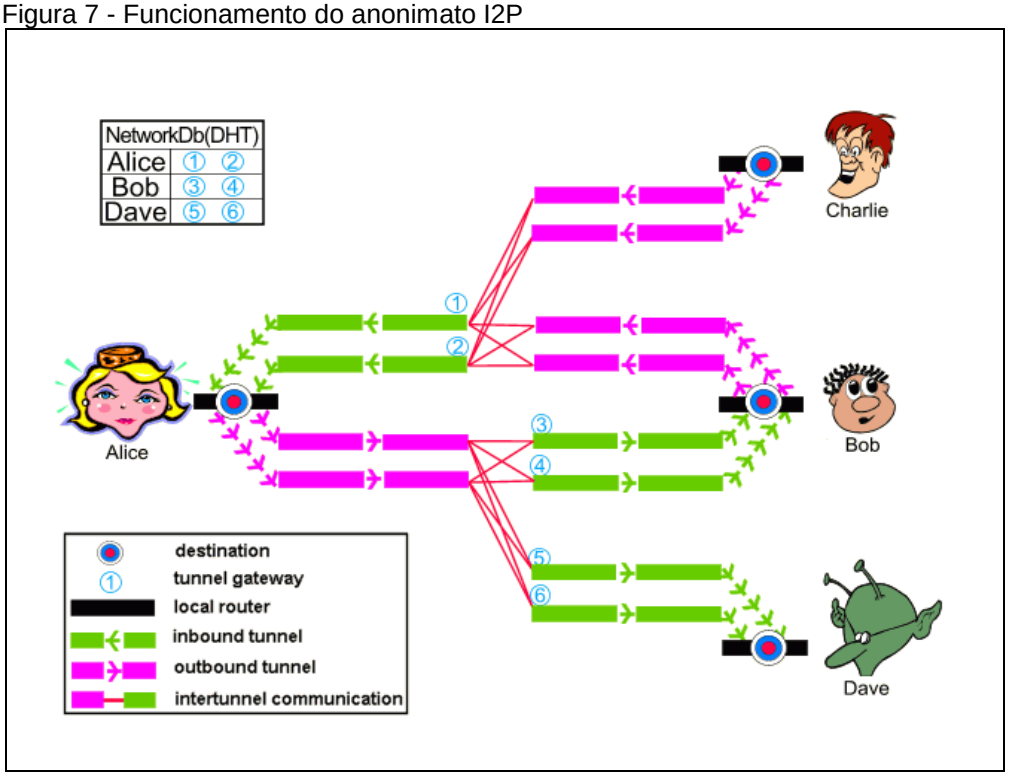
netDB contém todas as informações de cada ponto I2P, contato e cada execução de serviço público dentro da rede I2P (ZANTOUT e HARATY, 2011).

Ele é baseado em uma tabela de *hash* distribuída que pode conter várias entradas porém uma única saída baseada no algoritmo Kademlia, faz com que encontre o melhor túnel para o destino. As mensagens enviadas da rede I2P é criptografada de ponta a ponta usando criptografia de Garlic.

A criptografia de Garlic é análoga à criptografia de *onions*, com a disparidade de que múltiplas mensagens de dados podem estar contidas em uma única criptografia. De acordo com Ciancaglini (2013) uma única mensagem com a criptografia de Garlic, podem conter várias mensagens para diferentes destinatários com o roteador I2P. a rede I2P é formada por clientes (também chamado pares, roteador ou nós) executando o software I2P, permitindo aos aplicativos para se comunicar através da rede.

A parte central deste software é o roteador I2P. O roteador I2P é responsável pela manutenção das estatísticas dos clientes, executando operações criptográficas, construção de túneis, prestação de serviços e retransmissão mensagens. As aplicações dependem fortemente dos túneis construídos pelo roteador I2P dos clientes para permanecer anônimo, com isso, quanto maior quantidade de usuários conectados utilizando a rede I2P mais seguro o anonimato será.

Figura 7 - Funcionamento do anonimato I2P



Fonte: I2P Project (2017).

Na figura 7 os exemplos de usuários Alice, Bob, Dave, Charlie se comunicando através de um roteador I2P. Cada integrante tem dois túneis de entrada *inbound tunnel* e dois de saída *outbound tunnel*, nesta figura os túneis de entrada de Charlie e os de saída de Dave foram abolido desta imagem por questão de espaço. Sendo assim, quando Alice deseja enviar uma mensagem para Bob, ela utiliza seus túneis de saída. De acordo com a imagem a informação será encaminhada por túneis de saída para o Bob que aleatoriamente seguira pelos gateways 3 ou 4. Já a resposta de Bob para Alice a mensagem é encaminhada por um de seus dois túneis de saída para aleatoriamente os dois de entrada de Alice 1 ou 2 (I2P Project, 2017).

Nesta transmissão de informação anônima, tem-se um cuidado para os dados não serem surpreendidos, por Hackers, que estão ali esperando por apenas uma falha. Para isso Alice e Bob investem em segurança a ser visto.

4 SEGURANÇA DA INFORMAÇÃO

O uso da Internet cotidiana está mais evidente no grande segmento da população, certamente para estas pessoas, é difícil pressupor como seria a vida sem poder desfrutar das variedades dos conteúdos, informações, facilidades que é obtida através de intermédio de navegadores Web desta tecnologia. Estas pessoas ao usufruírem podem correr um grande risco relacionado ao uso da Internet, o primordial é que ela acredita que não corre riscos. Assim supondo que com a quantidade de pessoas conectadas simultaneamente e globalmente, alguém iria ter interesse em utilizar o seu computador para realizar um ataque, por exemplo, ou assentir-se que o seu nunca será localizado (RAMOS, 2008).

É exatamente o tipo de pensamento que os atacantes querem explorar, ao se sentirem seguros, acreditam que não precisam se prevenir. Este devaneio, lamentavelmente, costuma finalizar quando os primeiros problemas começam a acontecer. Ela pode estar sendo uma vítima de uma atividade maliciosa, por exemplo, estar compartilhando o processamento do seu computador sem sua permissão, para servir de ataques e repositórios de dados fraudulentos. Assim ajudando o atacante a esconder sua verdadeira identidade e localização (NBSO, 2017).

O primeiro passo que ela pode dar é a prevenção dos riscos mencionados com o uso da Internet. É estar informado que ela não tem nada de virtual. Tudo o que ocorre ou é executado através do intermédio na Internet é real. Os dados são reais assim como as pessoas com quem se interage. O mesmo acontece com as empresas, ao usuário passar as suas informações pessoais, como CPF, RG e cartões de crédito. Atualmente elas estão mudando drasticamente seu pensamento a respeito sobre a segurança da informação. Onde antes era visto como despesa hoje é um investimento.

Devido à grande abrangência dos sistemas, a ampliação nos números de usuários e das aplicações, consequente aumento das ameaças. A Segurança da Informação vem se tornando um processo cada vez mais importante dentro destas organizações, sendo assim, implantando as políticas de segurança (SÊMOLA, 2003).

4.1 POLÍTICAS DE SEGURANÇA

A política de segurança é o componente mais importante quando se referência sobre segurança em redes, e deve abranger desde a segurança física, lógica, privacidade e a legitimidade de software. Para funcionar corretamente, tudo tem que ser planejado, pois o importante não é apenas funcionar e sim funcionar bem e com segurança.

O intuito da política de segurança não é determinar procedimentos específicos de manipulação e proteção da informação, mas reivindicar os direitos e responsabilidades aos usuários que mourejam com essa informação. Ela determina o que deve ser feito e não como se fazer. Por exemplo, a empresa decreta que as senhas utilizadas nos sistemas internos devem, atender os requisitos de complexidade, ter a presença de um caractere especial, números e devem ter no mínimo oito caracteres (BARALDI, 2004).

Ela conduz a uma direção e mantem as ações do administrador da rede para elevar o nível de segurança e que com as ferramentas necessárias force com que seja cumprida estas exigências. Por exemplo, de acordo com a política de segurança, define que o sistema das estações sejam automaticamente bloqueadas após dez minutos de inatividade. Caso os usuários não estiverem de acordo com a mudança, ele será apoiado pela existência desta política de segurança, onde consta que esta regra deve existir. Isto é, não foi ele que definiu fazer a implantação da segurança e sim a empresa

As políticas devem ser divulgadas e apoiadas por todos os níveis da empresa. Porem muitas empresas esquecem de aplicar esta política, aplica sem planejamento ou acaba deixando em segundo plano. Até que os problemas começam a surgir, por exemplo, ataques de hackers. Resultando em custos elevadíssimos para sua resolução. O administrador da rede se preocupada em todos os possíveis níveis de segurança, ao contrário de um atacante, onde analisa e busca explorar apenas uma falha, seja ela, em hardwares, softwares ou nas redes (UCHÔA, 2005).

Os hackers são aqueles que utilizam o seu conhecimento para invadir os sistemas, sem o propósito de causar perdas às vítimas, mas sim, como um desafio às suas habilidades. Alguns informam até o local que está a falha. Já os crackers são aqueles que tem a intenção de prejudicar a vítima, causando os piores danos e

as vezes até irreversíveis.

As motivações para estes ataques são diversas. Dependendo do atacante pode ser apenas pelo aprendizado, fama, recompensa, vingança, espionagem ou curiosidade. Já as consequências também são diversas, tais como, o vazamento de informações, modificações de arquivos, corrupção de serviços, fazer com que a vítima passe trabalho, entre outras. Muitas empresas estão aplicando criptografias nos arquivos para sua maior segurança (NAKAMURA & GEUS, 2003).

4.2 CRIPTOGRAFIAS

A criptografia é uma ciência que foi construída com o intuito de embaralhar as informações de remetente para destinatário, onde todo o percurso e transporte desta informação será de forma totalmente segura. Somente o destinatário tem a chave secreta e acesso. Ela carrega a importância indispensável para a segurança da informação, servindo de base para diversas tecnologias e protocolos. A criptografia possibilita a integridade, a legitimidade e o segredo da informação (NAKAMURA & GEUS, 2003).

Diversas condições podem ser analisadas para efetuar a proteção apropriada da informação. Entre os principais estão: como será feita a geração das chaves, estrutura para a troca das chaves, quantidade de vezes para troca das chaves, tamanho das chaves e pôr fim a qualidade e eficiência do algoritmo e sua correta implementação (BERNSTEIN, 1997).

Um algoritmo criptográfico é considerado eficiente quando não existem quaisquer tipos de facilidade que permita a recuperação dos dados sem a utilização de ataques de força bruta. Caso venha acontecer, o número de chaves deve ser capaz de fazer com que os ataques se tornam inviáveis. Com o crescimento exponencial da propensão de processamento unido com o avanço da computação distribuída, geralmente utilizada por pessoas mal intencionadas, é imprescindível levar em conta o tempo no qual a informação deverá ficar protegida, assim utilizado um tamanho ideal da chave.

É possível utilizar a criptografia em diversos níveis de segurança, por exemplo, em senhas MD5, serviços e sistemas. Entre os tipos de criptografia para sistemas estão: *Shadow Password Suite*, *GNU Privacy Guard*, *RSA* e *DAS*, (SILVEIRA, 2009).

A criptografia pode ser utilizada para favorecer a comunicação em uma rede pública de forma segura, através da criação de túneis criptografados. Este túneis utilizam protocolos conhecidos como SSL ou SSH. Com a utilização do algoritmo criptográfico, mesmo que um invasor consiga tomar posse dos dados, ele não consegue acessá-lo ou abstrair informações.

Uma aplicação bem utilizada da criptografia pode ser vista nas redes privadas virtuais (VPN'S). Em uma VPN existe um túnel criptografado, por exemplo, entre um ponto A para o ponto B, ambos estão conectados simultaneamente porém utilizando um intermediário com uma rede pública, possibilitando comunicações seguras através de redes inseguras (UCHÔA, 2005).

4.3 PORTAS TCP E UDP

Todo computador ou dispositivo na Internet tem um número exclusivo atribuído a ele, chamado de endereço IP. Esse endereço IP é usado para reconhecer seu computador específico dentre os milhões de outros computadores conectados à Internet. Quando as informações são enviadas e recebidas pela Internet através de vários serviços abertos, por exemplo, um programa de e-mail, servidor de transferência de arquivos FTP ou até mesmo um software de download de vídeos e arquivos para este dispositivo, como eles podem estar funcionando simultaneamente sem entrar em conflito? Ele aceita essas informações usando portas TCP ou UDP (FERREIRA, 2013).

Duas analogias são feita para melhor entendimento, pode-se imaginar que o endereço IP é uma caixa de cabos e as portas são os diferentes canais da caixa de cabo. A empresa de cabeamento sabe como enviar o cabo para o decodificador de TV a cabo, com base em um número de série exclusivo associado a essa caixa (Endereço IP) e, em seguida, recebe os programas individuais em diferentes canais (Portas).

E a outra analogia, imagine que as duas partes do endereço IP, a parte relacionada à rede e a parte relacionada ao host, representam ao CEP de uma rua e ao número de um prédio. Um carteiro necessita apenas destas duas referências, para entregar uma carta. Porém, anexo ao prédio habitam diversas pessoas. O CEP e número do prédio só irão fazer a carta regressar até a portaria. E internamente no

prédio é necessário ter a posse do número do apartamento. É nesse momento que entram as ilustres portas TCP e UDP (MOTA, 2013).

Existem um total de 65.536 portas TCP e outras 65.536 portas UDP, que vão de 0 a 65.535 portas, sendo que, a maioria dos principais aplicativos tem uma porta específica que eles recebem e registram essas informações em uma organização chamada IANA onde lá fornece uma lista de aplicativos e as portas que eles correspondem no Registro da IANA. Com os desenvolvedores registrando as portas que seus aplicativos usam com a IANA, as chances de dois programas tentarem usar a mesma porta é mínima, assim reduzindo a causa de um conflito (MELO, 2017).

As portas TCP mais utilizadas conhecidas como WKP são as quais iniciam de 0 a 1023, que são reservadas para serviços mais conhecidos e utilizados, como servidores web, FTP, servidores de e-mail, compartilhamento de arquivos, etc. A porta 80, por exemplo, é reservada para uso de servidores web, enquanto a porta 21 é a porta padrão para servidores FTP.

A porta "0" é reservada, por isso não entra realmente na lista. Sendo que as portas que estiverem abertas indevidamente em um sistema operacional, podem acarretar problemas, por exemplo, sendo utilizadas por pessoas má intencionadas conhecidas como hackers, possibilitando uma invasão e roubo de informações. Essas portas TCP e UDP trabalham na camada 4 do modelo OSI, camada de transporte. A ser visto o fluxo de dados entre as portas (COMER, 2006).

4.4 FLUXO DE DADOS

Nas portas TCP, os dados são transportados transversalmente das conexões. Tudo inicia com o cliente remetendo o pacote SYN, que requisita a abertura da conexão. Em uma hipótese que a porta encontre-se fechada, o servidor devolve com um pacote RST e a comunicação finaliza. Eventualmente, por outro lado, se determinado servidor encontra-se disponível na porta pretendida um servidor web, por exemplo, logo ele corresponde com outro pacote SYN, seguido de um pacote ACK, informando que a porta está disponível e continua com a abertura da conexão (MORIMOTO, 2008).

O cliente responde nesse caso com outro pacote "ACK", o que disponibiliza oficialmente a conexão. Inicia assim a transferência dos dados, que são

estruturados em pacotes. O protocolo TCP/IP concede o uso de pacotes com até 64 Kbytes, mas são comumente usados pacotes com até 1500 bytes, que é a dimensão máxima de um frame Ethernet. Pacotes superiores podem ser transportados normalmente de lado a lado da rede, mas necessitam ser fragmentados, ou seja, fracionados em pedaços menores, com até 1500 bytes.

Para cada pacote recebido, a estação remete um pacote de validação e, eventualmente ocorra algum pacote se perca na camada de transporte, ela solicita a retransmissão. Cada pacote compreende 4 bytes extras com um código de CRC, que autoriza averiguar a integridade do pacote. É por meio dele que o cliente compreende cujo pacotes voltaram danificados (FERREIRA, 2013).

Posteriormente que todos os dados são difundidos, o servidor remete um pacote "FYN", comunicando que não tem mais dados a transmitir. O cliente responde com outro pacote "FYN" e a conexão é oficialmente encerrada.

A confiabilidade de comunicação é boa. Na ocasião em que a conexão está ruim, é normal ocorrerem perdas de pacotes e retransmissões, mas as corrupções são comumente ocasionadas pelo próprio software que está baixando um arquivo pelo repositório e não pelo protocolo. O contratempo é que todas estas regras, o torna as transferências mais lentas (COMER, 2016).

a) estação: SYN (solicita a abertura da conexão);
b) servidor: SYN (confirma o recebimento e avisa que a porta está disponível);
c) servidor: ACK (inicia a conexão);
d) estação: ACK (confirma);
e) estação: DATA (é enviado o pacote com a mensagem de texto);
f) servidor: OK (a confirmação, depois de verificar a integridade do pacote);
g) estação: FYN (solicita o fechamento da conexão);
h) servidor: FYN (confirma);
i) estação: FYN (confirma que recebeu a confirmação).

No decorrer do transporte dos dados, podem ocorrer ataques conhecidos como DOS no qual o atacante envia várias requisições SYN para um sistema alvo planejando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI. Assim conseguindo sobrecarregar e acessar algumas informações que contenha o pacote (ROSS; KUROSE, 2013).

4.5 PROCESSAMENTO E RECURSOS

Um computador é uma máquina composta por CPU, memória e dispositivos de entrada e saída capaz de sistematicamente coletar, manipular e prover resultados da utilização de dados para um ou mais propósitos. Por ser uma máquina composta de diversos circuitos e elementos eletrônicos, também é chamado de equipamento de processamento eletrônico de dados (STALLINGS, 2002).

A CPU é a elemento do computador que compreende e executa as instruções composta no software, a memória é forma de armazenamento (momentâneo ou permanecente) para que as informações apuradas ou processados sejam capazes de ser armazenadas. Os dispositivos são compostos por entradas e saídas. As entradas são dispositivos físicos que capturam os dados a serem processados, por exemplo, teclado e mouse. Os de saída são os resultados finais do processamento, por exemplo, monitores de vídeo e impressoras (TANEMBAUM, 2003).

O processamento de dados (manual ou automático) resulta em um objeto executado: a informação. Assim, os dados tem a necessidade de serem processados para que determinado resultado seja alcançado e tenha significado para um indivíduo ou para o próprio computador.

O computador processa os dados, conduzido por um conjunto de instruções, software, para fornecer decorrências completas com um miniatural de interferência humana.

Entre seus inúmeros proventos, pode-se citar:

a) extensa velocidade no processamento e disponibilidade de informações;
b) acuracidade na entrega das informações;
c) conformação para aplicação de tarefas repetitivas;
d) retenção de custos operacionais;
e) compartilhamento de dados.

O software mais conhecido é o sistema operacional Windows, é ele quem possibilita a interação com o computador e que transforma as ordens dos

dispositivos de entrada e saída ao mesmo. Sem um sistema operacional instalado em um conjunto de hardwares, computador, ele se torna inútil. Nele é possível instalar outros softwares e armazenar todos os dados em uma memória. Para a manutenção do mesmo ele grava todas alterações contidas no software, chamada de registros do Windows (MACHADO, 2007).

4.6 REGISTRO DO WINDOWS

Os computadores pessoais (PCs) baseados no sistema operacional Windows oferecem uma plataforma para interações de software significativas e complexas. No entanto, usos indisciplinados e compartilhamento de dados de configurações persistentes por programas do Windows tornaram os PCs mais vulneráveis.

O registro do Windows é um banco de dados hierárquico global, no qual as entradas são acessadas por chaves. Cada chave de registro tem um contexto de segurança anexado a ela, controlando o acesso à chave. Algumas chaves de registro armazenam informações confidenciais como o caminho para o executável agindo como um *shell* do usuário, a biblioteca a ser carregada por um programa, a identidade de um objeto do sistema operacional (GANAPATHI; WANG; WEN, 2004, tradução nossa).

Fazendo com que a administração torne organizada, viavel e mais facil. Por ele conter todos esses dados armazenado em um só lugar e através do painel de controle o usuario poder fazer alterações, ele acaba se tornando o componente mais vulnerável do sistema operacional Windows, mesmo que esteja atualizado com todos os virus ja existentes, ele fica exposto aos que estão sendo desenvolvidos posteriormente.

Se um adversário pode sobrescrever o conteúdo de uma chave sensível contendo o caminho de uma biblioteca ou executável, ele poderia fazer com que seu código fosse executado. Entender e desfazer os danos de um Registro causado por um virus, um usuario mal intencionado ou um *hacker*, é uma tarefa não trivial para o usuário comum. O problema é tão oneroso para os desenvolvedores de sistemas e aplicativos quanto para os usuários (GOVINDAVAJHALA; APPEL, 2006, tradução nossa).

5 TRABALHOS CORRELATOS

Para viabilizar este trabalho foram pesquisados alguns trabalhos na mesma área, porém não foi encontrado uma grande quantidade destes, mesmo com esta dificuldade foi possível o desenvolvimento de uma metodologia a ser aplicada. A grande parte dos trabalhos encontrados são em língua estrangeira, mas não foi empecilho para o bom entendimento.

5.1 SILK ROAD ANONYMOUS MARKET: UM ESTUDO DE CASO SOBRE O COMÉRCIO ANÔNIMO NA DEEP WEB

Desenvolvido em 2014 por Thayse Vasconcelos Hoffman como projeto final da Faculdade de Biblioteconomia e Comunicação, Relações Públicas da Universidade Federal do Rio Grande do Sul, em Porto Alegre, esta tese descreve um estudo de caso sobre o comércio anônimo na Deep Web.

O presente trabalho relata como é feito as comunicações entre os usuários que acessam a Silk Road, com o ponto de partida, o anonimato. Utilizando o software Tor Project para acessar a Deep Web juntamente com as tecnologias do anonimato, criptografias e como é feito o pagamento dos produtos comprados neste ambiente virtual, com o uso dos Bitcoins. E por fim ela conclui com este estudo de caso que o anonimato entre os usuários vendedores não decompõem a identidade e prestígio das práticas comunicacionais. (HOFFMAN, 2014, tradução nossa)

5.2 EM QUE MEDIDA A DEEP WEB AUMENTA A DIFUSÃO DE PODER

Desenvolvido em 2014 por Barbara Idaerla Santos Calderon como projeto final da Faculdade de Relações Internacionais da Universidade Federal de Santa Catarina, em Florianópolis, esta tese descreve em que medida a Deep Web aumenta a difusão de poder.

Inicialmente o trabalho descreve toda a bibliografia sobre a propagação do poder e a Deep Web. Ela efetuou o estudo de casos procedente do “submundo” da web, onde foram discutidos os grupos que por consequência obtiveram uma repercussão global. Conhecidos como Wikileaks, Anonymous, Silk Road e terrorismo islâmico jihadista. Onde ela analisou os resultados e as possíveis consequências, e se provou que a eficácia do uso das ferramentas para o acesso anônimo na Deep

Web se tornou capaz de passar despercebido pelos monitoramentos das instituições governamentais entre outras agencias. (CALDERON, 2014, tradução nossa)

5.3 O QUE A DEEP WEB PODE OFERECER ALÉM DA SURFACE WEB

Desenvolvido em 2013 por Barbara Carlos Henrique Aguiar dos Santos e Késsia Rita da Costa Marchi da Universidade Paranaense, em Paranavaí. Este artigo descreve o que a *Deep Web* pode oferecer além da *Surface Web*.

Inicialmente o trabalho propõe a explicação e demonstração do funcionamento da *Deep Web*, que é conhecida por ser uma web oculta e que seus sites não são indexados por motores de busca convencionais, se tornando anônimos e um atrativo para pessoas que cometem atividades ilícitas e cibercrimes. Porem este artigo visa demonstrar que não existe apenas este lado oculto na *Deep Web*, e sim conteúdos altamente relevantes e informações de livros, artigos científicos, filmes, jogos entre outros. E por fim provam que se usar de forma correta, o usuário será beneficiado pois há muitos conteúdos que dificilmente são encontrados na *Surface Web*, ao contrário da *Deep Web* (AGUIAR e MARCHI, 2013, tradução nossa).

6 METODOLOGIA

A metodologia aplicada é teórica e experimental, para a execução deste projeto, foi realizado a revisão bibliográfica de todos os materiais e temas abordados, logo após iniciou a fase do estudo para encontrar ferramentas, onde foi realizado a verificação das alterações ocorridas durante todas as etapas do processo, tais como, o monitoramento da instalação do software TOR e durante o uso, foi analisado os pontos de alteração de registro, quais possíveis registros foram criados e quais poderiam impactar na segurança do usuário, quais portas externas foram abertas ou não, análise de processamento quando o software está em utilização e o monitoramento das redes de entrada e saída efetuando analises para esses casos.

Dentre diversas ferramentas disponíveis na Internet para os testes práticos neste presente estudo, foram selecionadas as que abstraiam maiores resultados, analisam possíveis vulnerabilidades, acuracidade dos resultados e relatórios, tais como, a ferramenta para gestão de fluxo de dados Wireshark, análise de registro Regshot, monitoramento do processamento PCMark8 e a ferramenta para análise de portas abertas Nmap.

6.1 NMAP

O Nmap Network Scanning é uma ferramenta de código aberto disponível na internet de múltiplas faces. Ela é usada por milhões de pessoas para a descoberta de redes, portas, sistemas operacionais, administração e auditoria de segurança. Ela foi desenvolvido para digitalizar uma variedade de endereços host ou um intervalo de endereços IP, inserido na linha de comando e determinar quais endereços estão ativos. Examinará um intervalo de portas, que pode ser selecionável pelo usuário, para identificar quais os serviços que estão em execução no sistema operacional (LYON, 1997, tradução nossa).

O NMAP é um software livre oferecido sob os termos da GNU GPL (GNU GPL *General Public License*). Foi originalmente escrito para rodar no Linux, mas agora está disponível para várias plataformas.

O software Nmap foi desenvolvido por Gordon Lyon conhecido por Fyodor que é o proprietário da insecure.org. Procurando uma ferramenta para simplificar a

exploração da *Internet* ele se descreve como um hacker. Explorando redes, *hardwares* e *softwares* aos seus limites com programação de código aberto, disponibilizando a distribuição gratuita desde 1997.

Como todas as ferramentas de segurança, ela pode ser usada defensivamente, por um especialista ou gerente de rede, para identificar pontos fracos que precisam ser corrigidos, ou ofensivamente, por um invasor, investigando vulnerabilidades a serem exploradas (LYON, 1999, tradução nossa).

Assim que o sistema operacional do computador de destino for identificado, o invasor poderá iniciar seu esforço concentrado nas vulnerabilidades já conhecidas daquele SO juntamente as portas abertas para comprometê-lo. De acordo com Fyodor, ele descreve para os usuários sempre manterem o seu sistema operacional atualizado e para aplicar todas as correções de segurança que a plataforma disponibilizar.

Para a descoberta do tráfico de redes e análise de pacotes de redes foi utilizada a ferramenta Wireshark, possibilitando assim a verificação de possíveis vulnerabilidades.

6.2 WIRESHARK

O Wireshark é uma ferramenta de código aberto lançado sob os termos da Licença Pública Geral GNU para criar perfis de tráfego de rede e analisar pacotes. Ela é frequentemente chamada de analisador de rede, analisador de protocolo de rede ou *sniffer*. Ela permite que seja visto o que está acontecendo dentro da rede em um nível microscópico. É uma ferramenta que foi desenvolvida para Linux e atualmente recebe atualizações voluntárias de desenvolvedores pelo mundo, se tornando uma multi-plataforma. O desenvolvimento do projeto iniciou por Gerald Combs em 1998 (KUMAR E YADAV, 2015, tradução nossa).

O software anteriormente era conhecido como Ethereal, mas devido a problemas com marcas registradas o projeto foi renomeado para Wireshark em maio de 2006. O funcionamento dele em uma analogia, o analisador de pacotes de rede é como um dispositivo de medição usado para examinar o que está acontecendo dentro de um cabo de rede, assim como um voltímetro é usado por um eletricista para examinar o que está acontecendo dentro de um cabo elétrico, porem em um nível mais alto.

É uma ferramenta que apresenta diversas informações e que caindo em mãos erradas podem ser usada para espionagem. Uma organização que usa a ferramenta deve certificar-se de que possui uma política de privacidade claramente definida que explicita os direitos de indivíduos usando sua rede, concede permissão para detectar o tráfego para problemas de segurança e solução de problemas e estabelece as políticas da organização para obter, analisar e reter amostras de tráfego de rede (JAMES, 2009, tradução nossa).

Com o intuito de monitorar não apenas as redes, foi escolhido a ferramenta Regshot para analisar as alterações dos registros no Windows e sua possível vulnerabilidade após alterações.

6.3 REGSHOT

Regshot é uma ferramenta compacta e fácil de usar que disponibiliza ver o que as aplicações estão fazendo dentro do registro do Windows. E também ela pode ser usada para comparar a quantidade de entradas de registro que foram alteradas durante uma instalação ou uma alteração nas configurações do sistema.

Embora a maioria dos usuários de PC nunca precise fazer isso, é uma ótima ferramenta para solucionar problemas e monitorar o registro. Possibilitando visualizar e analisar uma possível abertura de vulnerabilidade no SO. Esta ferramenta também permite que você salve o conteúdo do registro do Windows, antes e depois, a fim de poder comparar quando quiser e poder (BUECHER, TIANWEI, XHMIKOSR, 2008, tradução nossa).

Regshot é um projeto de código aberto (LGPL) hospedado no SourceForge. Foi projetado e registrado em janeiro de 2001 por M. Buecher, Xhmikosr e Tianwei. Desde a sua criação, ele já foi modificado e atualizado inúmeras vezes para melhorar sua funcionalidade. Suportando apenas as linguagens em inglês e francês.

O objetivo deste software é comparar seu registro em dois pontos separados, criando uma imagem do registro antes de qualquer alteração no sistema e depois, ou quando os programas são adicionados, removidos e modificados.

6.4 PCMARK 8

A Futuremark é uma fornecedora respeitada de aplicativos benchmark para computadores. Seus benchmarks PCMark e 3DMark existem há quase 20 anos e fornecem uma boa indicação do desempenho do sistema para várias cargas de trabalho. A Futuremark lança o PCMark 10, sua sétima atualização para a série PCMark de benchmarks lançada pela primeira vez em 2002. Várias versões do PCMark foram lançadas. As pontuações não podem ser comparadas entre versões, em vez que cada uma inclui testes diferentes (BENCHMARK, 2018, tradução nossa).

O PCMark 8 é uma ferramenta desenvolvida pela UL (antiga Futuremark) para testar o desempenho de um PC no nível de sistema e componente. Na maioria dos casos, os testes na ferramenta PCMark 8 são projetados para representar cargas de trabalho típicas de usuários domésticos e de escritório. Ao executar produz uma pontuação com números mais altos indicando melhor desempenho.

Com base em aplicativos comerciais e de código aberto, mede o tempo de execução de extrações de código altamente representativas desses aplicativos e relatórios que refletem o desempenho geral do sistema, o desempenho da CPU, o desempenho do subsistema de memória, o desempenho do subsistema gráfico e o desempenho do subsistema de disco (SIBAI, 2008, tradução nossa).

Os resultados que ele traz é satisfatório e exato. Esses resultados ajudam a entender as características de desempenho e a orientar melhorias futuras no design do processador, memória e disco. Facilitando também analisar o processamento no decorrer do uso do computador no exato momento

Do outro ponto de vista, este software também pode ajudar as empresas a exigir um nível mínimo de desempenho para os sistemas que eles esperam comprar. O PCMark 8 mede o desempenho do sistema usando cargas de trabalho baseadas em aplicativos e atividades do mundo real que refletem o uso de PCs modernos em um ambiente de escritório

A carga de trabalho de inicialização do aplicativo envolve a medição do tempo necessário para iniciar vários programas de complexidade variável, como o navegador da web, o processador de textos e programa de manipulação de imagens.

Os testes de navegação na Web envolvem a navegação de um site de mídia social, compras on-line, navegação em mapas, reprodução de vídeo (H.264 e VP9 em resoluções de 1080p e 4K) e uma página da Web estática.

A carga de trabalho de videoconferência lida com conferências one-on-one de baixa qualidade (codificação e decodificação 720p30 H.264, bem como detecção de face executada em um dispositivo ou CPU OpenCL disponível), bem como conferência em grupo de alta qualidade 1080p30 codificação H.264 e 3x decodificação 720p30 H.264, bem como detecção de face (BENCHMARK, 2018, tradução nossa).

7 APRESENTAÇÃO E ANÁLISE DOS DADOS

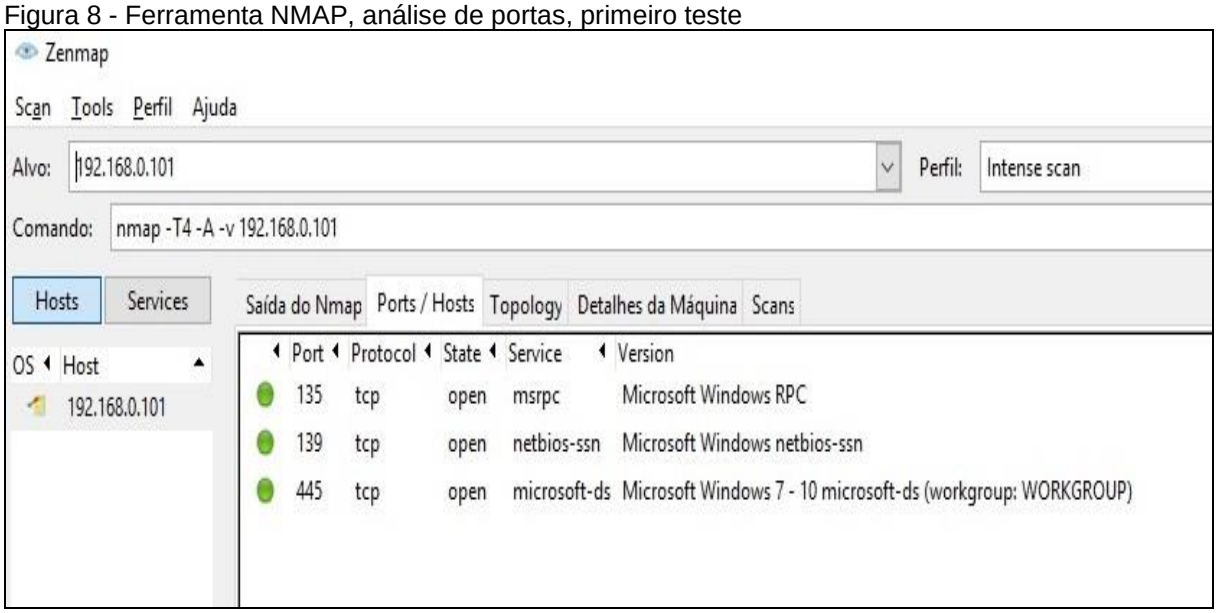
Após o levantamento dos requisitos das possíveis vulnerabilidades a serem analisadas com a utilização de ferramentas e recursos necessários para execução da metodologia, esse tópico relata os resultados alcançados com a utilização, testes e análises feitas com as ferramentas.

Os testes executados foram em um computador Windows com 6GB de memória RAM, 500GB de HD e processador Intel Core i3. A rede é doméstica e passa por modem e roteador. A quantidade de amostra para realização dos teste foram de 10 vezes a partir de cada vulnerabilidade a ser abordada.

Partindo da análise de vulnerabilidades a primeira avaliada foi a de Portas Abertas, utilizando a ferramenta NMAP. Na sua interface principal de fácil interação, foi realizado os testes de verificação nas 65.536 portas de rede no sistema operacional Windows antes de instalar o software TOR, que permite acesso a Deep Web. No Alvo, o software solicita o endereço IP do computador, a ser inserido pelo usuário.

Com este endereço IP e com o equipamento operando em uma rede foi realizado a primeira varredura.

Figura 8 - Ferramenta NMAP, análise de portas, primeiro teste



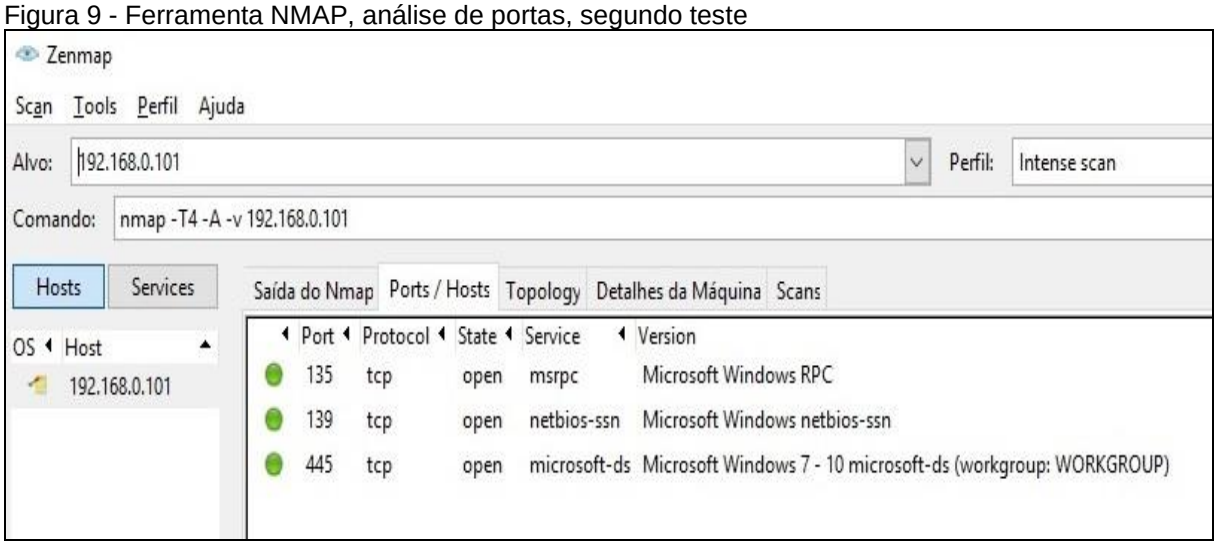
Fonte: Do autor

A figura 8 demonstra que ao efetuar a análise destas portas, foi possível constatar que havia três portas abertas, sendo elas, 135, 139 e 445 todas TCP. Ao

realizar a pesquisa sobre estas portas e serviços ali mostradas, consta que, para o funcionamento do sistema operacional Microsoft Windows, essas portas já são habilitadas por padrão.

Após o teste realizado, deu-se início ao próximo teste. No teste seguinte, com o software TOR instalado, executando e acessando a Deep Web na máquina, foi submetido a uma nova varredura.

Figura 9 - Ferramenta NMAP, análise de portas, segundo teste

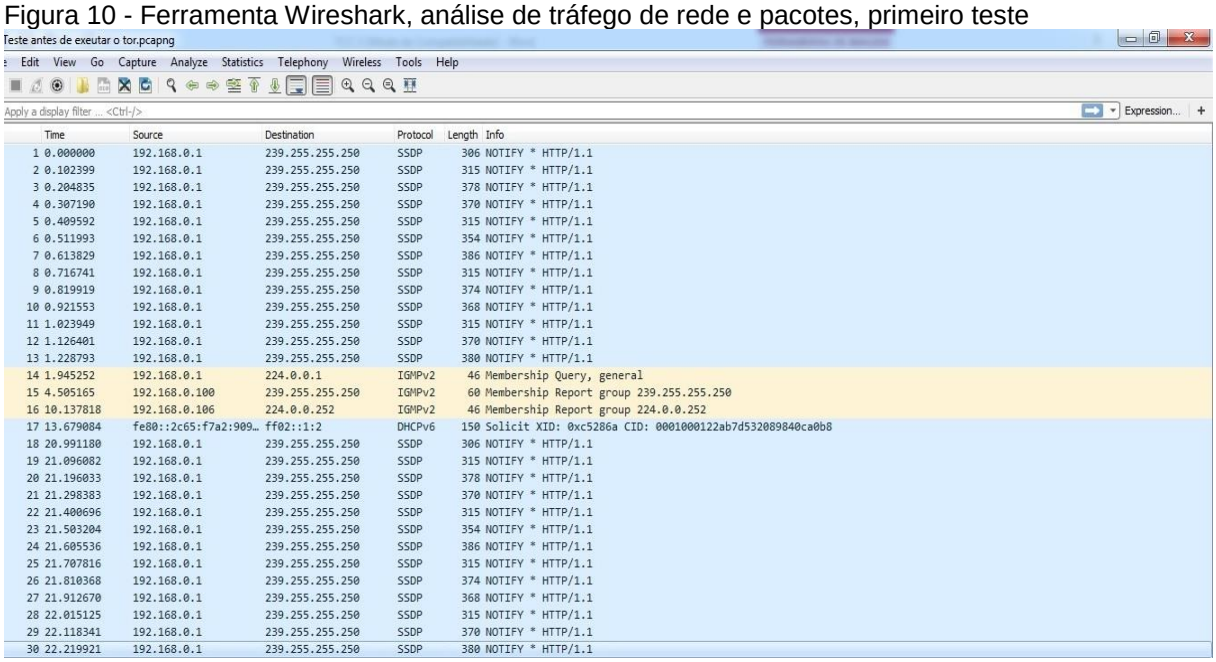


Fonte: Do autor

Na figura 9 com os resultados obtidos, foi possível afirmar que mesmo após a instalação e execução do software TOR e acessando a *Deep Web*, não houve alterações significativas de portas abertas para uma possível vulnerabilidade no sistema operacional, além das padrões da Microsoft Windows que já foram verificadas no teste anterior.

Partindo da análise de vulnerabilidades de portas, a segunda avaliada foi a de tráfego de rede e pacotes. Utilizando a ferramenta Wireshark com seus relatórios e interfaces práticas, foi possível monitorar todo o fluxo de entrada e saída da rede antes da execução da ferramenta TOR.

Figura 10 - Ferramenta Wireshark, análise de tráfego de rede e pacotes, primeiro teste

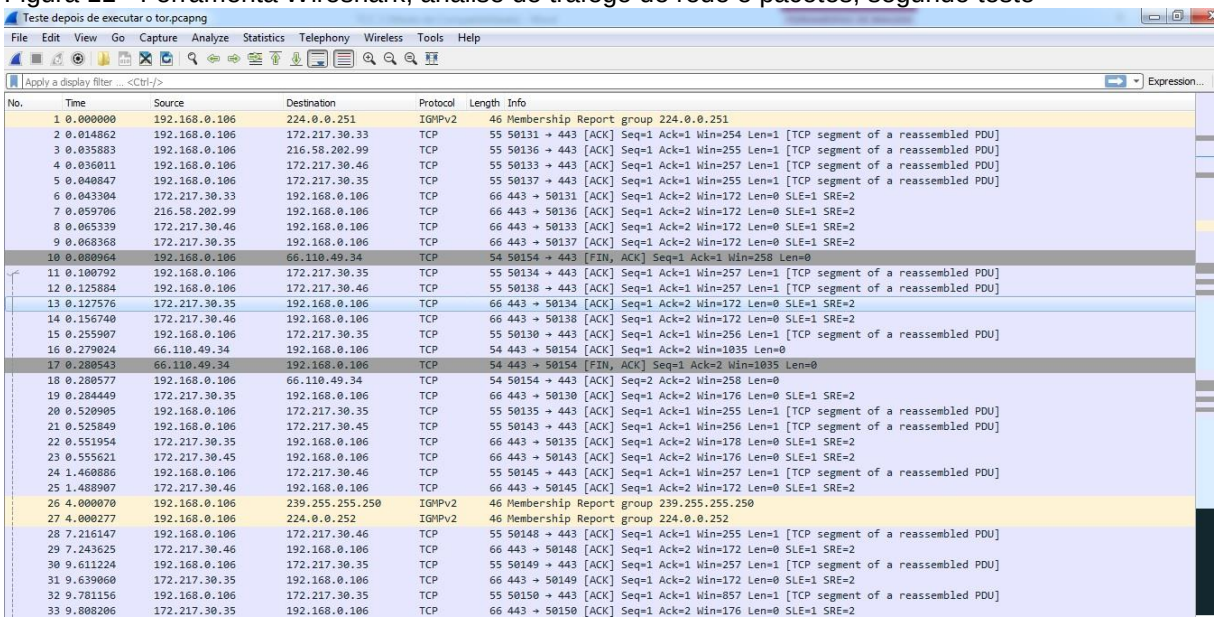


Fonte: Do autor

Na Figura 10 apresenta a interface principal da ferramenta Wireshark, com todo fluxo de dados da rede após fazer a primeira varredura. Em análise linha por linha, é possível observar todos os endereços IP e fluxo de dados de sincronismo e resposta de cada pacote, onde, não demonstra nenhuma vulnerabilidade no sistema operacional Microsoft Windows.

Assim, dando início ao próximo teste. Após executar e acessar a Deep Web com software TOR, foi referido uma nova varredura.

Figura 11 - Ferramenta Wireshark, análise de tráfego de rede e pacotes, segundo teste



Fonte: Do autor

A figura 11 é possível observar que constam alguns pedidos de finalização de sincronização e confirmações, porém, não houve nenhuma alteração significativa para resultar em uma vulnerabilidade.

Partindo da análise do fluxo de dados e pacotes, a terceira avaliada foi a de desempenho, memória e processamento com a ferramenta PCMark 8, com sua interface gráfica que apresenta resultados significativos e exatos no momento do uso, assim tornando viável.

O primeiro teste foi feito antes de executar a ferramenta TOR e acessar a *Deep Web*.

Figura 12 - Ferramenta PCMark8, análise de desempenho, primeiro teste

Fonte: Do autor

A Figura 12 demonstra o estado atual do computador, resultando em um *score* de 2.017, com vídeo Intel HD *Graphics* 3000 mobile e processador Intel Core i3-2348M CPU. Após este primeiro teste, foi submetido a uma nova análise com a ferramenta TOR executada e acessando a *Deep Web*.

Figura 13 - Ferramenta PCMark8, análise de desempenho, segundo teste

Fonte: Do autor

Na Figura 13 é possível observar uma pequena diferença de *score* do teste comparado ao anterior. Ao ser analisado, constatou que a diferença é tão baixa que resultou no esforço do computador para manter a ferramenta em execução, com isso não justificando uma possível vulnerabilidade de compartilhamento de processamento.

Partindo da análise de vulnerabilidades de desempenho, memória e processamento com, a quarta e última avaliada foi a de alterações de registro no sistema operacional Microsoft Windows. Utilizando a ferramenta Regshot disponibilizando seu recurso de capturar todos os registros e chaves antes e todos os registros após a instalação e execução, foi possível comparar os dois e analisar todas alterações obtidas antes da instalação e depois da instalar e execução da ferramenta TOR.

Figura 14 - Ferramenta Regshot, análise de alterações no registro do sistema operacional Windows

Created with Regshot 1.9.0 x64 ANSI

Comentários:

Dia/hora:2018/4/17 15:14:03 , 2018/4/17 15:16:34

Computador:DESKTOP-Q0PALV2 , DESKTOP-Q0PALV2

Usuário:vitor , vitor

Chaves adicionadas:61

HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html\OpenWithList
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\e667d6a9_0
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\e667d6a9_0\{219ED5A0-9CBF-4F3A-B927-37C9E5C5F14F}
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\3
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\4
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\5
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\2\3
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\0
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\0\0
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\12\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\18
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\18\ComDlg
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\18\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\18\Shell
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\19
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\19\ComDlg
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\19\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\19\Shell
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20\Shell
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\21
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\21\Shell
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\22
HKU\S-1-5-21-312894696-1307014817-3141829016-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\22\Shell
HKU\S-1-5-21-312894696-1307014817-3141829016-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\3
HKU\S-1-5-21-312894696-1307014817-3141829016-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0\0\0\4

Fonte: Do autor

Na figura 14 mostra todas as alterações feitas em comparação de antes e depois de instalar a ferramenta TOR. Houve um total de alterações de 287 registros, sendo eles 61 chaves adicionadas, 182 valores adicionados e 44 valores modificados. Em análise de todas as chaves adicionadas e modificadas, não constou nenhuma alteração significativa para resultar em uma vulnerabilidade.

8 CONCLUSÃO

Para o processamento de análise sucedeu algumas dificuldades, um lapso na literatura existente sobre o tema abordado por se tratar de uma nova área nas pesquisas, mas a contar do material encontrado pode-se desenvolver esse estudo.

O presente estudo teve como objetivo analisar as possíveis vulnerabilidades de um computador sob o ponto de vista do usuário ao acessar a *Deep Web*. A partir desde ponto, abordou-se o lado histórico da Internet, e em especial o anonimato na *Deep Web*. Foi abordada a instalação da ferramenta TOR para realizar o acesso a *Deep Web*, seu funcionamento e características que a diferenciam da *Surface Web*, cujo os conteúdos são indexado por mecanismos de busca padrão, como Google, Yahoo e Bing, por conseguinte, visível ao usuário médio comum.

Aproveitando-se do anonimato, do dinamismo dos sites, da criptografia, de não conter leis aplicáveis até o momento da pesquisa, a *Deep Web* atrai um grande número de usuários que tem intenções duvidosas podendo agir com privacidade, efetuando atividades ilícitas como, tráfico de órgãos, tráfico de drogas, tráfico de armas, pedofilia, assassinos de aluguel entre outros.

Nesse intermédio dos usuários da *Deep Web*, atraiu também os usuários que apenas evitam as ferramentas de monitoramento, poder político e social, conhecidos como curiosos, leitores e jornalistas, que publicam acontecimentos em livros e vídeos que por razão das diretrizes impostas na *Surface Web* não pode ser indexada e publicada nos mecanismos de busca padrão.

Abordou-se nas histórias sobre segurança da informação e criptografias, especialmente ao navegar na *Deep Web*, pois o uso da Internet trouxe o maior acesso de comunicação globalizada já existente, tornou-se cotidiana nas vidas das pessoas, algumas precavidas e outras que sente-se seguras e optam por não utilizar nenhum método de prevenção, evidentemente pessoas má intencionadas aproveitam dessa situação para invadir o computador da vítima, assim tornando-se um hospedeiro de dados fraudulento e fazendo com que o processamento seja compartilhado e tornando a identidade do real invasor seja escondida.

Concluiu-se que com o uso das ferramentas NMAP, Wireshark, Regshot, PCMARK8 foi possível realizar testes práticos necessários de verificação de portas

abertas, fluxo de dados de entrada e saída na rede, processamento e alterações e adições de chaves no registro do Windows antes e depois obtiveram os resultados negativos para possíveis vulnerabilidades, desde a instalação até a navegação na *Deep Web*.

Aos usuários iniciantes para acessar a *Deep Web*, aconselha-se que utilizem todos os métodos de segurança disponíveis, mesmo que com todos os teste práticos já realizados apresentarem resultados negativos.

Os objetivos específicos e gerais foram alcançados com sucesso e os resultados documentados podem ajudar na decisão de como acessar a *Deep Web* em segurança.

Necessita-se e espera-se que, no futuro, mais pesquisas e estudos sejam desenvolvidos sobre a segurança da informação e a *Deep Web*, proporcionando aos usuários maiores informações e segurança nesse submundo virtual anônimo.

REFERÊNCIAS

ARAÚJO, W.F. ***We open governments***: Análise de discurso do ciberativismo praticado pela organização WikiLeaks. 2013. 207 f. Dissertação (mestrado)- Universidade Feevale, Novo Hamburgo, 2013. Disponível em:< http://www.academia.edu/7046139/We_open_governments_An%C3%A1lise_de_discurso_do_ciberativismo_praticado_pela_organiza%C3%A7%C3%A3o_WikiLeaks>. Acesso em: 05 out. 2017.

BARALDI, P. **Gerenciamento de riscos:** a gestão de oportunidades, a avaliação de riscos e a criação de controles internos nas decisões empresariais. Rio de Janeiro: Elsevier/Campus, 2004.

BENCHMARK. **PCMark 10 benchmark: The complete benchmark for the modern office.** Abril. 2018 Disponivel em: <https://benchmarks.ul.com/pcmark10> Acesso em: 07 jun. 2018.

BERGMAN, Michael. **White paper: the Deep Web: surfacing hidden value**. Journal of electronic publishing. Michigan: University of Michigan Library, vol.7, Ed.1, 2001.

BERNSTEIN, Peter L. Desafio aos Deuses 3ª ed. Rio de Janeiro: Campus, 1997.

CASTELLS, Manuel. **A galáxia da Internet:** reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: J. Zahar, 2003.

CASTELLS, Manuel; CARDOSO, Gustavo. **The Network Society: From Knowledge to Policy**. Washington, DC: John Hopkins Center for Transatlantic Relations, 2005.

CIANCAGLINI, Vicenzo et al. **A Trend Micro Research Paper: Deep Web and cybercrime: it's not all about TOR.** Cupertino: Trend Micro. 2013.

CLARKE, Ian. **Um Sistema de Recuperação e Recuperação de Informação Descentralizada Distribuída**. Julho de 1999. Disponível em: < http://www.freenetproject.org/ > Acesso em: 25 out. 2017.

COMER, Douglas E. **Redes de Computadores e Internet.** 6. ed. Rio Grande do Sul: Bookman, 2016.

COMER, Douglas E. Interligação de Redes com TCP/IP. V. 1. 5.ed. São Paulo: Campus, 2006.

CONRAD,Bernd; SHIRAZI, Fatemeh. **A Survey on Tor and I2P: The Ninth International Conference on Internet Monitoring and Protection.** Germany, 2014. Disponível em:<http://www.i2pproject.net/_static/pdf/icimp_2014_1_40_30015.pdf> . Acesso em: 02 nov. 2017.

DOTSON, Jeremy. **HTTP vs. HTTPS: What's the Difference?**. v. 1, jun. 2007. Disponível em <https://biztechmagazine.com/article/2007/07/http-vs-https>. Acesso em: 05 out. 2017.

Dr. KUMAR, Mahesh, YADAV, Rakhi. **"TCP & UDP PACKETS ANALYSIS USING WIRESHARK"** International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

FERREIRA, Rubem E. **Novatec. Linux: Guia do Administrador do Sistema**. 2.ed. São Paulo: Novatex, 2013.

FREENET, Project: **anonymity online**. Disponível em:< https://freenetproject.org >. Acesso em: 25 out. 2017.

GANAPATHI, Archana. WANG, Yi-Min. LAO, Ni. WEN, Ji-Rong. **Why PCs Are Fragile and What We Can Do About It: A Study of Windows Registry Problems.** MSR-TR, 2004.

GOVINDAVAJHALA, Sudhakar. APPEL, Andrew W. Windows Access Control Demystified. Princeton University, Janeiro de 2006. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.1930&rep=rep1&type=pdf> Acesso em: 06 jun. 2018.

I2P Project: **A Gentle Introduction to How I2P Works.** Fev**.** 2003 Disponível em: < http://www.geti2p.org/how_intro > Acesso em: 28 nov. 2017.

JAMES, A. K., BARTON P. M., EDUARDO, C., ELISA, H. **"First principles vulnerability assessment".** 2009**.** Disponível em: <http://research.cs.wisc.edu/mist/VA.pdf> Acesso em: 21 maio. 2018.

LÉVY, P. **A inteligência coletiva: por uma antropologia do ciberespaço.** 4. ed. São Paulo: Loyola, 2003.

LIMA, Lucas. **Iceberg.** São Paulo: 6 jul. 2017. Disponível em: < **https://www.profissas.com.br/como-conseguir-trampo-exterior-guia-pratico/iceberg/ >** Acesso em: 28 nov. 2017.

LYON, Gordon. **"The Art of Port Scanning"** Phrack Magazine v. 7, p. 11-17, 1997. Disponível em: <http://www.insecure.org/nmap/p51-11.txt> Acesso em: 21 maio. 2018.

LYON, Gordon**. "Remote OS detection via TCP/IP Stack FingerPrinting"** Abril. 10, 1999. Disponível em: < http://www.insecure.org/nmap/nmap-fingerprinting-article.html > Acesso em: 21 maio. 2018.

MACHADO, Francis B. **Arquitetura de sistemas operacionais**. 4º ed. Rio de Janeiro: LTC, 2007.

MARTINS, Caio Arthur Lopes da Silva; SILVA, Maria Helena Barriviera e. **A dualidade da *Deep Web***. E-f@tec, Garça, v. 3, n. 2, p.1-7, 2013. Disponível em:

<http://www.fatecgarca.edu.br/revista/Volume3/artigos_vol3/Artigo_16.pdf>. Acesso em: 11 out. 2017.

MELO, Sandro. **Exploração de Vulnerabilidades: Em Redes TCP/IP**. 3.ed. São Paulo: Alta Books, 2017.

MOTA, João E. Filho. **Análise de Tráfego Em Redes TCP/IP - Utilize tcpdump na análise de tráfegos em qualquer sistema operacional.** 1.ed. São Paulo: Novatex, 2013.

MORIMOTO, Carlos E. **Redes, guia prático: hardware, o guia definitivo**. 2. ed. São Paulo: GHD Press e Sul Editores, 2008.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício. Segurança de redes: em ambientes cooperativos. 2. ed. São Paulo: Futura, 2003.

NASCIMENTO, Barbara Luiza Coutinho do. **Liberdade de expressão, honra direito e privacidade na internet: a evolução de um conflito entre direitos fundamentais**. 2009. 95 f. Monografia (Especialização) - Curso de Direito, Escola de Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2009.

NBSO. Uso Seguro da Internet março. 2017. Disponível em:< https://cartilha.cert.br/uso-seguro/>. Acesso em: 20 nov. 2017.

PALACIOS, Bryan. **Surface Web vs. Deep Web**. RITS n.9 La Paz nov. 2014. Disponível em:<http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442014000100007&script=sci_arttext&tlng=es>. Acesso em: 02 out. 2017.

PEDERSON, Steve. **Understanding the Deep Web in 10 Minutes**, Bright Planet Deep Web Intelligence, 2013.

PISAREWICZ, Piotr. **Privacidade na Rede Aberta**. 2013. 86 f. TCC (Graduação) - Curso de Computação, Universidade de Brasília, Brasília, 2013.

POMPÉO, Wagner Augusto; SEEFELDT, João Pedro. **Nem tudo está no Google: deep web e o perigo da invisibilidade.** In: Congresso Internacional de Direito e Contemporaneidade. Anais..., Santa Maria: UFSM, 2013. Disponível em:<http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 02 out. 2017.

RAMOS, A. (Org.). **Security Officer 1:** guia oficial para formação de gestores em Segurança da Informação. 2. ed. Porto Alegre: Zouk, 2008.

ROSS, Keith W; KUROSE, Jim. **Redes de Computadores e A Internet - Uma Abordagem Top-Down.** 6.ed. São Paulo: Pearson, 2013.

SÊMOLA, Marcos. Gestão da Segurança Informação Uma visão executiva. 2ª ed. Rio de Janeiro, RJ: Campus, 2003.

SIBAI, Fadi N. **Evaluating the performance of single and multiple core processors with PCMARK®05 and benchmark analysis.** v.35. Nova York: Newsletter, 2008.

SILVEIRA, Sérgio Amadeu. **Redes cibernéticas e tecnologias do anonimato. Comunicação & Sociedade**, v. 1, p. 113-134, 2009.

STALLINGS, Willian. **Arquitetura e Organização de Computadores: Projeto para o Desempenho**. Tradução de Carlos Camarão de Figueiredo e Lucília de Figueiredo. São Paulo: Prentice Hall, 2002.

TANEMBAUM, Andrew S. **Sistemas Operacionais Modernos**. 2ª ed. Tradução de Ronaldo A.L. Gonçalves e Luis A. Consularo. São Paulo: Prentice Hall, 2003.

TOR Project: **anonymity online**. Disponível em:< https://www.torproject.org/>. Acesso em: 18 out. 2017.

UCHÔA, Joaquim Quinteiro. **Segurança Computacional**. Lavras: UFLA/FAEPE, 2005. (Curso de Pós Graduação “Latu Sensu” (Especialização) a Distância em Administração em Redes Linux).

ZANTOUT, Bassam; HARATY, Ramzi. **I2P Data Communication System: The Tenth International Conference on Networks.** Lebanon, 2011. Disponível em:<http://csm.beirut.lau.edu.lb/~rharaty/pdf/IC15.pdf>. Acesso em: 02 nov. 2017.

APENDICE A – ARTIGO

ESTUDO DE VULNERABILIDADES NO USO DA DEEP WEB SOB O PONTO DE VISTA DO USUÁRIO

Vitor Medeiros[1], Valter Blauth Junior[2]

[1]Academico do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma - SC

[2]Professor do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – SC

Vitormed95@live.com, valterblauth@unesc.net

Abstract. *The main objective of this research was to demonstrate in a practical and theoretical way the possible vulnerabilities in which the user and his computer are exposed during the navigation in the Deep Web and the vast problem when accessing the Deep Web. Because it is a wide network of anonymity, in some situations the release of various security items from the computer may be able to compromise the security and user information. The methodology applied in the present work was practical and theoretical with the use of tools, in order to analyze possible open ports, registry of the Microsoft Windows operating system, and processing and data flow in the network.*

Resumo. *Esta pesquisa teve como objetivo principal demonstrar de forma prática e teórica as possíveis vulnerabilidades, em que o usuário e seu computador se expõe durante a navegação na Deep Web e o vasto problema ao acessar a Deep Web. Por se tratar de uma ampla rede de anonimato, em algumas situações podem ocorrer a liberação de diversos itens de segurança do computador, capaz de comprometer a segurança e as informações do usuário. A metodologia aplicada no presente trabalho foi prática e teórica com a utilização de ferramentas, a fim de analisar possíveis portas abertas, registro do sistema operacional Microsoft Windows, processamento e fluxo de dados na rede.*

1. Introdução

A Deep web conhecida como Internet profunda hospeda sites que por motivos de necessidade de anonimato não são indexados pelos motores de busca da Internet. Sendo assim representam uma porta aberta para atividades ilícitas e cibernéticas.

Os usuários comumente utilizam a chamada Surface Web ou "web rasa" onde segundo Pompéo e Seefeldt (2013) a coletânea de páginas são facilmente encontradas por mecanismos de buscas, diferente da Deep Web que resume as páginas e por necessidade de anonimato não pertencem a esses provedores, não podendo assim serem listados como resultados. É a definição de indexar as páginas nos mecanismos de buscas que a distinguem como ela será encontrada ou não por esses serviços. Cada página da rede contém padrões que a registram em servidores como Yahoo! e Google.

Para ter acesso a Deep Web existem várias ferramentas, sendo a The Onion Router (TOR) uma destas. De acordo com (CIANCAGLINI, 2013) o TOR é uma tecnologia gratuita e pode

ser obtido e utilizado por qualquer usuário e para acesso a Deep Web através da Internet. Esta rede permite comunicações anônimas através de nódulos voluntários que são responsáveis por traçar uma rota de pedidos criptografados para que o trânsito de dados possa passar despercebido por ferramentas de monitoramento.

Sendo assim, durante a sua instalação e funcionamento podem ocorrer a liberação de diversos itens de segurança tais como portas de acesso, controle da máquina, processamento e outros. Com o intuito de aprofundar os conhecimentos sobre a Deep Web utilizando esta ferramenta, o presente estudo pretende demonstrar a vulnerabilidade da máquina e do usuário através de experimento prático e teórico desde a instalação até a navegação propriamente dita.

2. Deep Web

De acordo com Pompéo e Seefeldt, “a expressão Deep Web foi criada por Michael K. Bergman, fundador do programa Bright Planet, software especializado em coletar, classificar e procurar conteúdo nessa esfera da web.” (POMPÉO; SEEFELDT, 2013, p.440).

A Deep Web conhecida como “web oculta”, preza o anonimato de seus usuários representando assim uma porta aberta para a realização de atividades ilícitas como: drogas, prostituição, pornografia, pedofilia, contrabando de mercadorias, materiais radioativos, tráfico de órgãos humanos, organização de jogos de azar, conter documentos do governo, sequestros dentre outros cibercrimes. Ainda não há tecnologia que possa tornar os seres humanos físicos invisíveis, mas é possível ser anônimo e, de certa forma, "invisível", na Internet, o software The Onion Router e navegando na web que é conhecido como a Internet profunda (BERGMAN, 2001).

Toda informação pesquisada mais profundamente na Deep Web é possível encontrar, não havendo decepções. Ao acessar esta profundeza deve-se tomar muito cuidado, por ser anônimo e conter páginas que por algum motivo não respeitam as regras solicitadas. Elas se tornam páginas de web não indexadas por provedores de busca, isto é, em uma requisição de informação no Google por exemplo, ele não irá conseguir obter a informação a respeito do hiperlink da página Deep Web e não conseguirá acessá-la (BERGMAN, 2001).

Diversas analogias são feitas para representar a dimensão da Deep Web, uma delas é a analogia feita com o mar, em que se faz referência a uma pessoa que está nadando, consegue visualizar apenas a superfície da água, mas que, com os devidos equipamentos de mergulho, pode emergir e descobrir um mundo que antes era invisível. O mesmo acontece na web com poucos recursos, apenas com navegadores os usuários acessam a superfície, porém sem os instrumentos precisos de maneira alguma conseguirá chegar à profundeza.

Por fim, existe outra relação que faz citação a um grupo de pescadores em um navio em alto mar. Quando jogam uma rede de pesca na área superficial de um mar, a probabilidade de pescarem peixes é muito pequena se comparada com a mesma rede jogada em maior profundidade.

A Deep Web é conhecida como Internet profunda e anônima, por vasto conteúdos ilícitos e de cibercrimes. Comumente utilizada por pessoas “usuários” mal intencionados. Sendo assim, o potencial de informações na Deep Web não se dá apenas por conteúdos ilícitos ou cibercrimes. Como afirmam Martins e Silva (2013) fica a escolha do usuário como será feito a escolha dos assuntos no qual se propõe encontrar nesta profundidade da rede.

O usuário está focado em encontrar documentos, informações científicas, livros e fatos não publicados por terem uma alta censura que possuem no acesso da Surface Web, seja porque determinados arquivos ou informações que estão sendo buscado, encontram-se mais ao final

da indexação dos mecanismos de busca convencionais, ou seja, porque tal conteúdo está pouco difundido na rede (BERGMAN, 2001).

Ele terá uma abrangência maior e uma grande chance de conseguir encontrar os conteúdos e arquivos na Internet profunda de uma forma ágil. Essa agilidade se interpreta em qualidade, pois, conforme dito anteriormente, ele conseguirá encontrar o que se propôs a buscar. Cabe destacar que por não haver a necessidade de se respeitar uma lei em vigor no que diz respeito à este espaço cibernético, diversos conteúdos e arquivos estão disponíveis integralmente, basta apenas utilizar os recursos corretos.

O Infomine é um mecanismo de busca específico para conteúdo de bibliotecas universitárias norte-americanas, entre elas a Universidade da California; o Intute permite acesso ao conteúdo de todas as universidades da Inglaterra; o Complete Planet dá acesso a assuntos diversos, como militares, comidas ou meteorologia para agricultores; o IncyWincy possui busca por imagens; o DeepWebTech, permite acesso a temas como medicina, negócios e ciências; o Scirus é direcionado para assuntos científicos, como jornais, homepages de cientistas, materiais didáticos e patentes; o TechXtra é direcionado para a área de exatas, como matemática, engenharia e computação. [...] Há aqueles que usam a Web Invisível para armazenar informações que precisam gerar tráfego, como por exemplo, resultados parciais de pesquisas, e o simples armazenamento de bases de dados organizacionais que não estão sendo utilizadas no momento. (MARTINS; SILVA, 2013, p.4).

A Deep Web é pelo menos 400-500 vezes o tamanho da Surface Web. Está crescendo continuamente, e isso significa que novas fontes da Deep Web também estão crescendo. Para acessar esta Internet profunda utiliza-se diferentes softwares que deixa o usuário anônimo na Internet, o mais conhecido The Onion Router (PEDERSON, 2013).

3. Segurança da Informação

O uso da Internet cotidiana está mais evidente no grande segmento da população, certamente para estas pessoas, é difícil pressupor como seria a vida sem poder desfrutar das variedades dos conteúdos, informações, facilidades que é obtida através de intermédio de navegadores Web desta tecnologia. Estas pessoas ao usufruírem podem correr um grande risco relacionado ao uso da Internet, o primordial é que ela acredita que não corre riscos. Assim supondo que com a quantidade de pessoas conectadas simultaneamente e globalmente, alguém iria ter interesse em utilizar o seu computador para realizar um ataque, por exemplo, ou assentir-se que o seu nunca será localizado (RAMOS, 2008).

É exatamente o tipo de pensamento que os atacantes querem explorar, ao se sentirem seguros, acreditam que não precisam se prevenir. Este devaneio, lamentavelmente, costuma finalizar quando os primeiros problemas começam a acontecer. Ela pode estar sendo uma vítima de uma atividade maliciosa, por exemplo, estar compartilhando o processamento do seu computador sem sua permissão, para servir de ataques e repositórios de dados fraudulentos. Assim ajudando o atacante a esconder sua verdadeira identidade e localização (NBSO, 2017).

O primeiro passo que ela pode dar é a prevenção dos riscos mencionados com o uso da Internet. É estar informado que ela não tem nada de virtual. Tudo o que ocorre ou é executado através do intermédio na Internet é real. Os dados são reais assim como as pessoas com quem se interage. O mesmo acontece com as empresas, ao usuário passar as suas informações pessoais, como CPF, RG e cartões de crédito. Atualmente elas estão mudando drasticamente seu pensamento a respeito sobre a segurança da informação. Onde antes era visto como despesa hoje é um investimento.

4. Metodologia

A metodologia aplicada é teórica e experimental, para a execução deste projeto, foi realizado a revisão bibliográfica de todos os materiais e temas abordados, logo após iniciou a fase do estudo para encontrar ferramentas, onde foi realizado a verificação das alterações ocorridas durante todas as etapas do processo, tais como, o monitoramento da instalação do software TOR e durante o uso, foi analisado os pontos de alteração de registro, quais possíveis registros foram criados e quais poderiam impactar na segurança do usuário, quais portas externas foram abertas ou não, análise de processamento quando o software está em utilização e o monitoramento das redes de entrada e saída efetuando analises para esses casos.

Dentre diversas ferramentas disponíveis na Internet para os testes práticos neste presente estudo, foram selecionadas as que abstraiam maiores resultados, analisam possíveis vulnerabilidades, acuracidade dos resultados e relatórios, tais como, a ferramenta para gestão de fluxo de dados Wireshark, análise de registro Regshot, monitoramento do processamento PCMark8 e a ferramenta para análise de portas abertas Nmap.

5. Resultados Obtidos

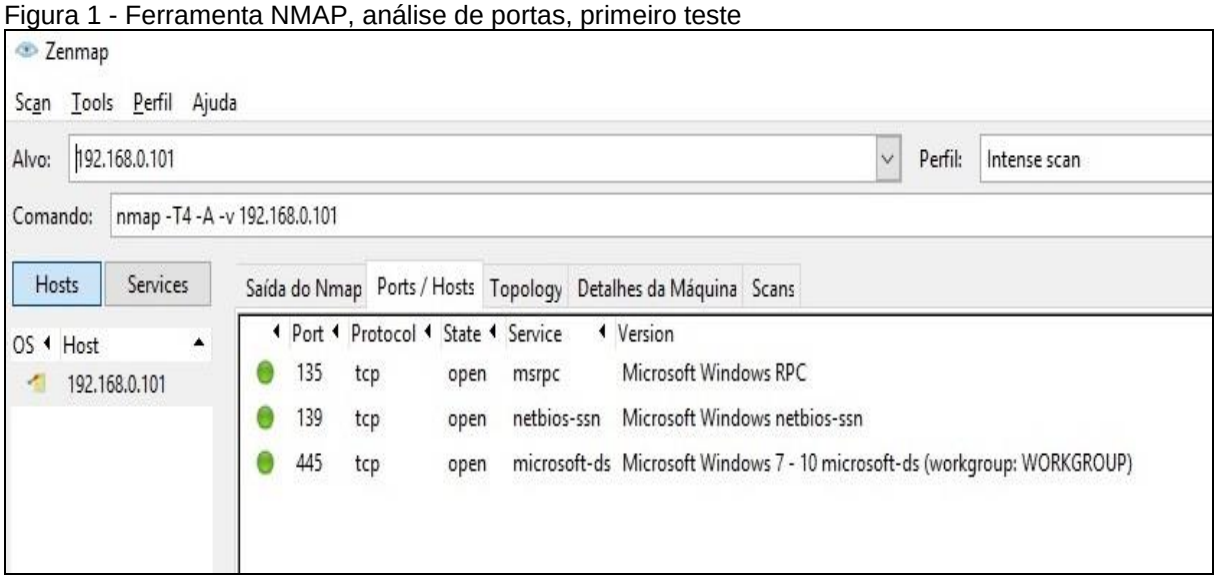
Após o levantamento dos requisitos das possíveis vulnerabilidades a serem analisadas com a utilização de ferramentas e recursos necessários para execução da metodologia, esse tópico relata os resultados alcançados com a utilização, testes e análises feitas com as ferramentas.

Os testes executados foram em um computador Windows com 6GB de memória RAM, 500GB de HD e processador Intel Core i3. A rede é doméstica e passa por modem e roteador. A quantidade de amostra para realização dos teste foram de 10 vezes a partir de cada vulnerabilidade a ser abordada.

Partindo da análise de vulnerabilidades a primeira avaliada foi a de Portas Abertas, utilizando a ferramenta NMAP. Na sua interface principal de fácil interação, foi realizado os testes de verificação nas 65.536 portas de rede no sistema operacional Windows antes de instalar o software TOR, que permite acesso a Deep Web. No Alvo, o software solicita o endereço IP do computador, a ser inserido pelo usuário.

Com este endereço IP e com o equipamento operando em uma rede foi realizado a primeira varredura.

Figura 1 - Ferramenta NMAP, análise de portas, primeiro teste

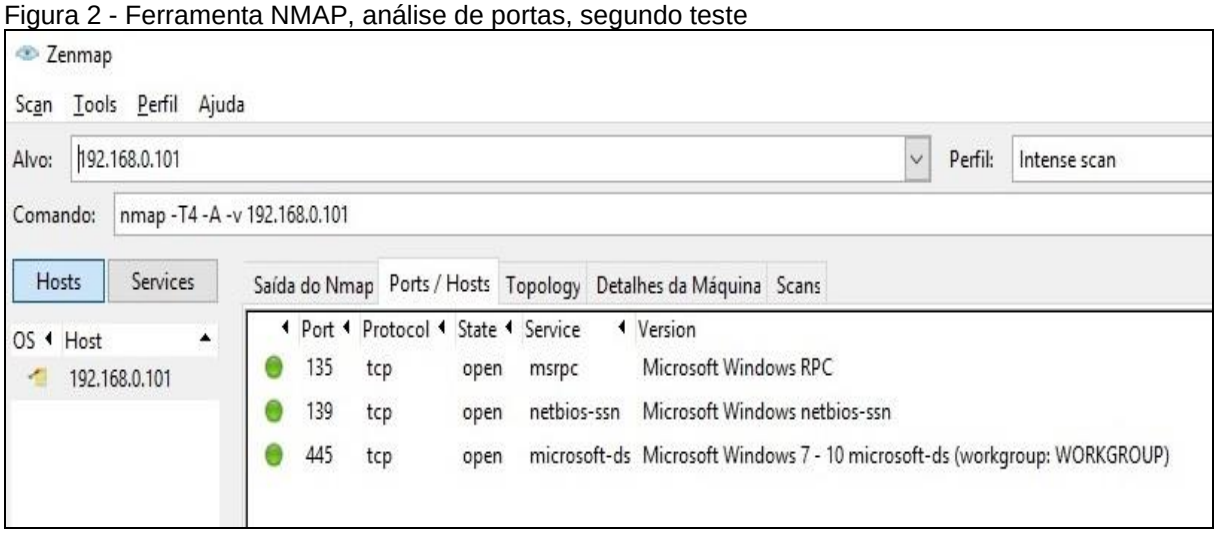


Fonte: Do autor

A figura 1 demonstra que ao efetuar a análise destas portas, foi possível constatar que havia três portas abertas, sendo elas, 135, 139 e 445 todas TCP. Ao realizar a pesquisa sobre estas portas e serviços ali mostradas, consta que, para o funcionamento do sistema operacional Microsoft Windows, essas portas já são habilitadas por padrão.

Após o teste realizado, deu-se início ao próximo teste. No teste seguinte, com o software TOR instalado, executando e acessando a Deep Web na máquina, foi submetido a uma nova varredura.

Figura 2 - Ferramenta NMAP, análise de portas, segundo teste



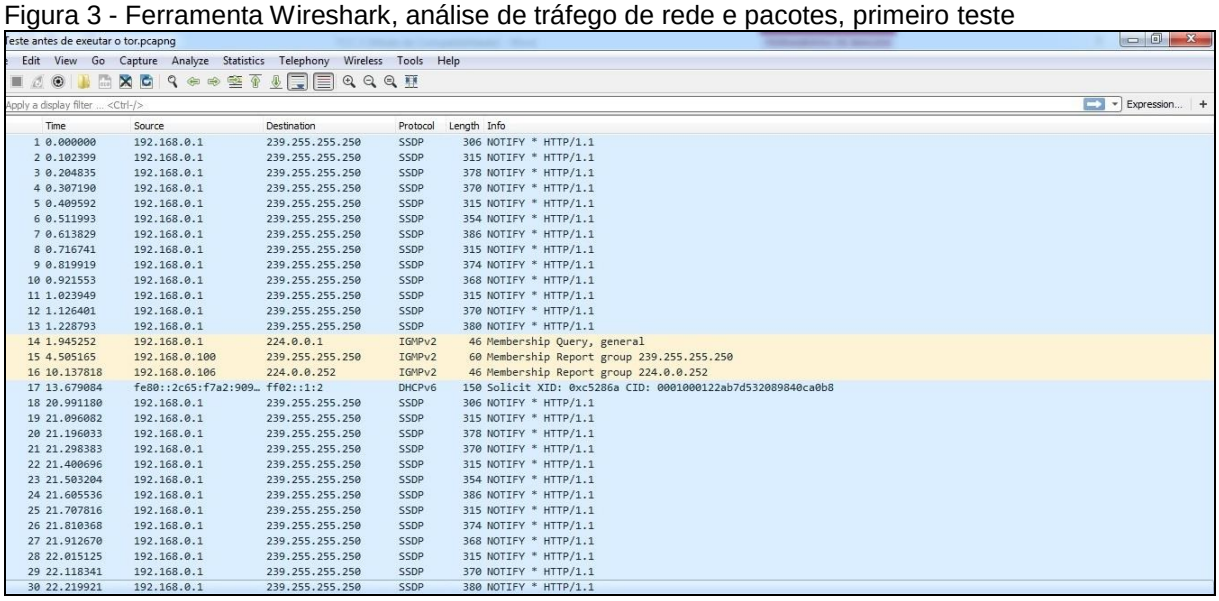
Fonte: Do autor

Na figura 2 com os resultados obtidos, foi possível afirmar que mesmo após a instalação e execução do software TOR e acessando a *Deep Web*, não houve alterações significativas de portas abertas para uma possível vulnerabilidade no sistema operacional, além das padrões da Microsoft Windows que já foram verificadas no teste anterior.

Partindo da análise de vulnerabilidades de portas, a segunda avaliada foi a de tráfego de rede e pacotes. Utilizando a ferramenta Wireshark com seus relatórios e interfaces práticas, foi

possível monitorar todo o fluxo de entrada e saída da rede antes da execução da ferramenta TOR.

Figura 3 - Ferramenta Wireshark, análise de tráfego de rede e pacotes, primeiro teste

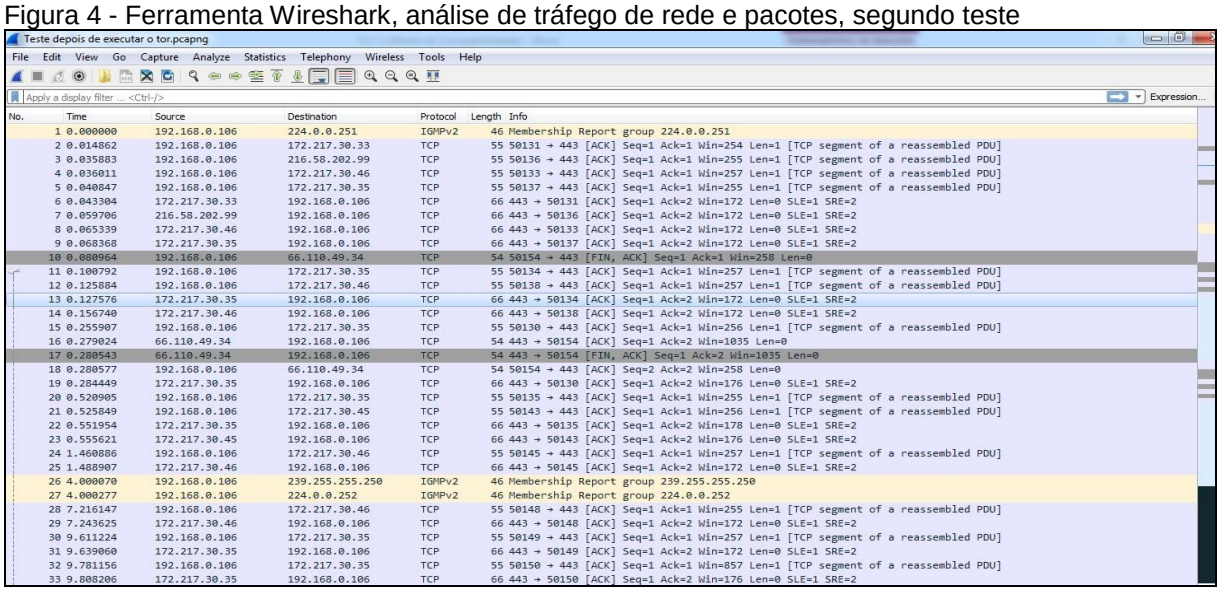


Fonte: Do autor

Na Figura 3 apresenta a interface principal da ferramenta Wireshark, com todo fluxo de dados da rede após fazer a primeira varredura. Em análise linha por linha, é possível observar todos os endereços IP e fluxo de dados de sincronismo e resposta de cada pacote, onde, não demonstra nenhuma vulnerabilidade no sistema operacional Microsoft Windows.

Assim, dando início ao próximo teste. Após executar e acessar a Deep Web com software TOR, foi referido uma nova varredura.

Figura 4 - Ferramenta Wireshark, análise de tráfego de rede e pacotes, segundo teste



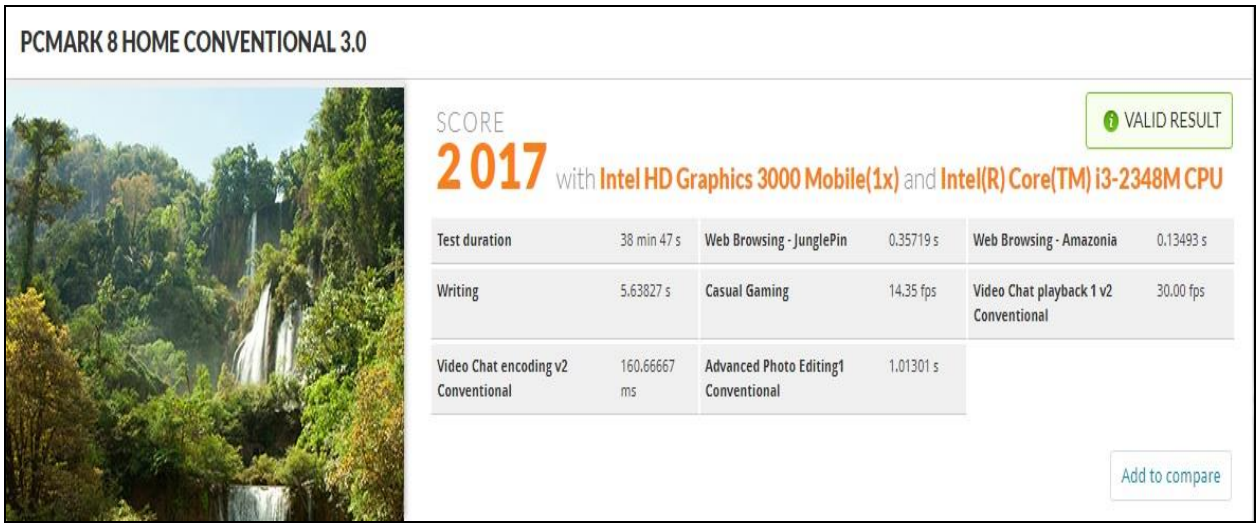
Fonte: Do autor

A figura 4 é possível observar que constam alguns pedidos de finalização de sincronização e confirmações, porém, não houve nenhuma alteração significativa para resultar em uma vulnerabilidade.

Partindo da análise do fluxo de dados e pacotes, a terceira avaliada foi a de desempenho, memória e processamento com a ferramenta PCMark 8, com sua interface gráfica que apresenta resultados significativos e exatos no momento do uso, assim tornando viável.

O primeiro teste foi feito antes de executar a ferramenta TOR e acessar a *Deep Web*.

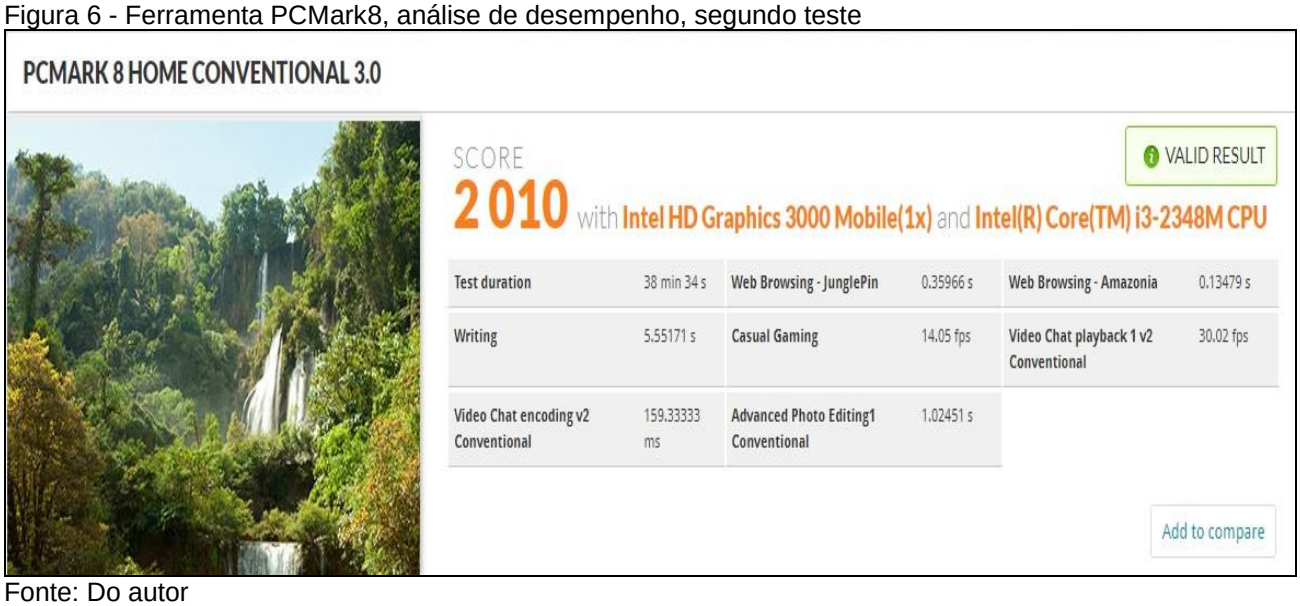
Figura 5 - Ferramenta PCMark8, análise de desempenho, primeiro teste



Fonte: Do autor

A Figura 5 demonstra o estado atual do computador, resultando em um *score* de 2.017, com vídeo Intel HD *Graphics* 3000 mobile e processador Intel Core i3-2348M CPU. Após este primeiro teste, foi submetido a uma nova análise com a ferramenta TOR executada e acessando a *Deep Web*.

Figura 6 - Ferramenta PCMark8, análise de desempenho, segundo teste

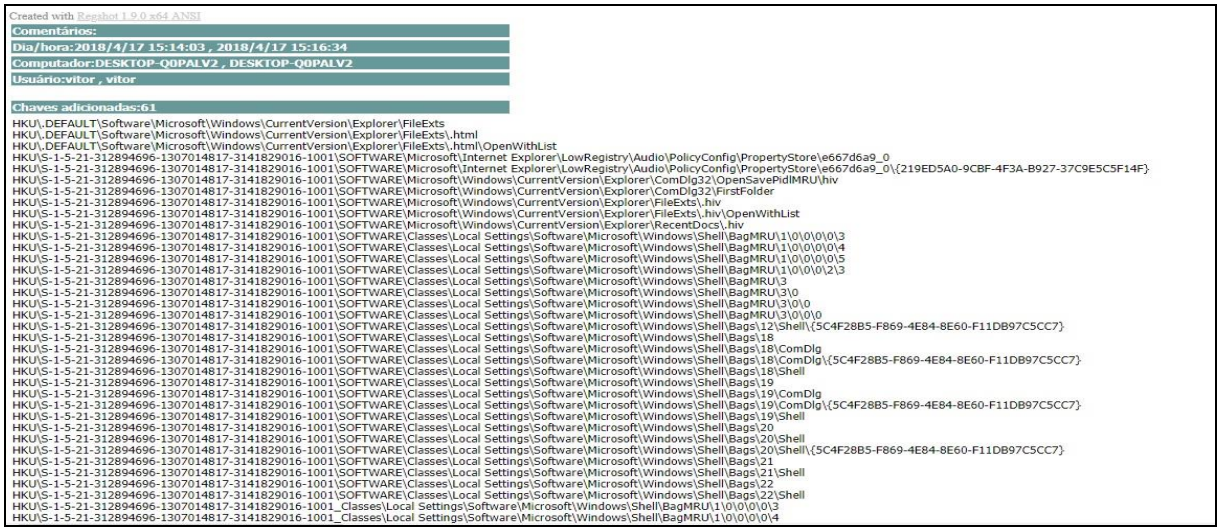


Fonte: Do autor

Na Figura 6 é possível observar uma pequena diferença de *score* do teste comparado ao anterior. Ao ser analisado, constatou que a diferença é tão baixa que resultou no esforço do computador para manter a ferramenta em execução, com isso não justificando uma possível vulnerabilidade de compartilhamento de processamento.

Partindo da análise de vulnerabilidades de desempenho, memória e processamento com, a quarta e última avaliada foi a de alterações de registro no sistema operacional Microsoft Windows. Utilizando a ferramenta Regshot disponibilizando seu recurso de capturar todos os registros e chaves antes e todos os registros após a instalação e execução, foi possível comparar os dois e analisar todas alterações obtidas antes da instalação e depois da instalar e execução da ferramenta TOR.

Figura 7 - Ferramenta Regshot, análise de alterações no registro do sistema operacional Windows



Fonte: Do autor

Na figura 7 mostra todas as alterações feitas em comparação de antes e depois de instalar a ferramenta TOR. Houve um total de alterações de 287 registros, sendo eles 61 chaves adicionadas, 182 valores adicionados e 44 valores modificados. Em análise de todas as chaves adicionadas e modificadas, não constou nenhuma alteração significativa para resultar em uma vulnerabilidade.

6. Conclusão

Para o processamento de análise sucedeu algumas dificuldades, um lapso na literatura existente sobre o tema abordado por se tratar de uma nova área nas pesquisas, mas a contar do material encontrado pode-se desenvolver esse estudo.

O presente estudo teve como objetivo analisar as possíveis vulnerabilidades de um computador sob o ponto de vista do usuário ao acessar a Deep Web. A partir desde ponto, abordou-se o lado histórico da Internet, e em especial o anonimato na Deep Web. Foi abordada a instalação da ferramenta TOR para realizar o acesso a Deep Web, seu funcionamento e características que a diferenciam da Surface Web, cujo os conteúdos são indexado por mecanismos de busca padrão, como Google, Yahoo e Bing, por conseguinte, visível ao usuário médio comum.

Aproveitando-se do anonimato, do dinamismo dos sites, da criptografia, de não conter leis aplicáveis até o momento da pesquisa, a Deep Web atrai um grande número de usuários que tem intenções duvidosas podendo agir com privacidade, efetuando atividades ilícitas como, tráfico de órgãos, tráfico de drogas, tráfico de armas, pedofilia, assassinos de aluguel entre outros.

Nesse intermédio dos usuários da Deep Web, atraiu também os usuários que apenas evitam as ferramentas de monitoramento, poder político e social, conhecidos como curiosos, leitores e jornalistas, que publicam acontecimentos em livros e vídeos que por razão das diretrizes impostas na Surface Web não pode ser indexada e publicada nos mecanismos de busca padrão.

Abordou-se nas histórias sobre segurança da informação e criptografias, especialmente ao navegar na Deep Web, pois o uso da Internet trouxe o maior acesso de comunicação globalizada já existente, tornou-se cotidiana nas vidas das pessoas, algumas precavidas e outras que sente-se seguras e optam por não utilizar nenhum método de prevenção, evidentemente pessoas má intencionadas aproveitam dessa situação para invadir o computador da vítima, assim tornando-se um hospedeiro de dados fraudulento e fazendo com que o processamento seja compartilhado e tornando a identidade do real invasor seja escondida.

Concluiu-se que com o uso das ferramentas NMAP, Wireshark, Regshot, PCMARK8 foi possível realizar testes práticos necessários de verificação de portas abertas, fluxo de dados de entrada e saída na rede, processamento e alterações e adições de chaves no registro do Windows antes e depois obtiveram os resultados negativos para possíveis vulnerabilidades, desde a instalação até a navegação na Deep Web.

Aos usuários iniciantes para acessar a Deep Web, aconselha-se que utilizem todos os métodos de segurança disponíveis, mesmo que com todos os teste práticos já realizados apresentarem resultados negativos.

Os objetivos específicos e gerais foram alcançados com sucesso e os resultados documentados podem ajudar na decisão de como acessar a Deep Web em segurança.

Necessita-se e espera-se que, no futuro, mais pesquisas e estudos sejam desenvolvidos sobre a segurança da informação e a Deep Web, proporcionando aos usuários maiores informações e segurança nesse submundo virtual anônimo.

Referencias

BERGMAN, Michael. White paper: the Deep Web: surfacing hidden value. Journal of electronic publishing. Michigan: University of Michigan Library, vol.7, Ed.1, 2001.

CIANCAGLINI, Vicenzo et al. A Trend Micro Research Paper: Deep Web and cybercrime: it's not all about TOR. Cupertino: Trend Micro. 2013.

MARTINS, Caio Arthur Lopes da Silva; SILVA, Maria Helena Barriviera e. A dualidade da Deep Web. E-f@tec, Garça, v. 3, n. 2, p.1-7, 2013. Disponível em: <http://www.fatecgarca.edu.br/revista/Volume3/artigos_vol3/Artigo_16.pdf>. Acesso em: 11 out. 2017.

NBSO. Uso Seguro da Internet março. 2017. Disponível em:< https://cartilha.cert.br/uso-seguro/>. Acesso em: 20 nov. 2017.

PEDERSON, Steve. Understanding the Deep Web in 10 Minutes, Bright Planet Deep Web Intelligence, 2013.

POMPÉO, Wagner Augusto; SEEFELDT, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Anais..., Santa Maria: UFSM, 2013. Disponível em:<http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 02 out. 2017.

RAMOS, A. (Org.). Security Officer 1: guia oficial para formação de gestores em Segurança da Informação. 2. ed. Porto Alegre: Zouk, 2008.