**INTRODUÇÃO**

Hacktivismo é entendido como uma manipulação de códigos que tem o propósito de fazer algum ataque ativista, geralmente os ataques são direcionados a mídia, meios de comunicação, governos, etc. Esse tipo de ativismo é frequente nos dias de hoje.

No Brasil houve vários ataques Hacktivista, mas a maioria deles ocorrem em época de eleição. Esses ataques ocorrem de todos os lados e sempre visam atrapalhar os candidatos da eleição.

As consequências desses ataques podem ser maiores do que aparentam, causando atraso e vários informações ou até mesmo a perca dessas informações, também pode ocorrer casos de vazamento de informações importantes de algumas pessoas.

Em nosso país ocorrem diversos ataques hacktivistas, mas não encontramos uma maneira fácil de visualizar, a frequência, localidade, os grupos responsáveis e motivos por trás desses ataques.

O objetivo deste trabalho será a criação de visualização de dados georreferenciados para o melhor entendimento dos ataques hacktivistas que ocorrem no Brasil.

**METODOLOGIA**

Foi feito um levantamento de dados sobre o Hacktivismo no Brasil, apresentando informações sobre ataques hacktivistas, detalhando: ano, motivo, local e prejudicados.

Os dados foram recolhidos a partir de postagens em blogs, redes sociais, jornais e artigos. Foram validados com base em buscas e comparações entre diversas publicações sobre o mesmo ataque.

Esses dados foram inseridos em **10** colunas **(id, site, uf\_descricao, local\_ataque, prejudicado, feita\_por, datahora\_ataque, hackers, descricao, datahora\_publicacao)** em uma planilha no Excel versão 2016. Essa planilha foi importada no Power BI Desktop versão 2.69 (Ferramenta que possibilita a criação do mapa). A planilha foi importada pela sequência de funções: **Obter dados**, **Excel**, **selecionar planilha**, **abrir**, **selecionar as tabelas** e **carregar** (Caminho executado no Power BI).

No projeto do Cisco Packet Tracer foi criado um projeto a partir de dois trabalhos, o trabalho “Enterprise Network Design in CISCO Packet Tracer (6.1.1)” ([DHAREDDY](https://www.youtube.com/channel/UCjLoPI87whBDSBvmjgBLh6w), [Srinivas](https://www.youtube.com/channel/UCjLoPI87whBDSBvmjgBLh6w), 2014) e o trabalho “Cisco Packet Tracer - Configuración de RFID y TRIP SENSOR (IOT)” (LUGO, Guillermo, 2018). Para isso no Cisco Packet Tracer, foi clicado em file e open sample, em seguida foi aberto o projeto do Srinivas Dhareddy, encima deste projeto foi seguido os passos do vídeo de Guillermo Lugo para a segurança do servidor com sensores.

Os arquivos do projeto no Cisco Packet Tracer, dados recolhidos, vídeo demonstrando a solução do cisco foram subidos para o Github, para isso foi criado um repositório no Github. Em seguida foi executado no sistema operacional Linux foi aberto o terminal e executado os comandos: “cd ” e “git clone https://github.com/brennocg/Hacktivismo.git”. Com isso uma pasta Hacktivismo foi criada na pasta home e então a pasta foi aberta e os arquivos foram movidos de forma manual para dentro da pasta, ou seja, puxando e arrastando. Após isso vamos atualizar o repositório do Github, então no terminal foi executado os seguintes comando: “git add \*”, “git commit -m "Atualização do documento"”, “git push” e em seguida o usuário e senha do Github, para fins de segurança do repositório.

**RESULTADOS**

Foi criado um mapa buscando sobrepor e sinalizar as informações de forma dinâmica e objetiva. Esse mapa contém diversas informações sobre cada ataque, possibilitando filtrar ataques por estado e visualizar de forma detalhada.

Link do mapa: <http://abre.ai/hacktivismo-redes-e-computadores>

Visualizando todas as informações adquiridas a partir da coleta de dados que feita, constatamos que todos ataques foram feitos derrubando o servidor por acesso externo com o ataque comumente chamado de “ping da morte” ou "Denial of Service". Esse tipo de ataque é quando um único pacote de dados com um formato inesperado é capaz de travar o sistema operacional inteiro. Para prevenir esses ataques recomendamos que sempre a empresa contrate serviços de nuvem de empresas confiáveis como os serviços oferecidos pela AWS, pois assim existe a certeza de segurança contra esse tipo de ataques e outros tipos que existem.

E para a segurança interna, também recomendamos que a empresa contrate sempre empresas de alta confiabilidade, pois sempre é preciso de muito conhecimento de segurança quando o assunto é rede de corporativa. No cenário governamental por exemplo, existem informações extremante valiosas que não podem vazar, desse modo é essencial para isso uma rede de alta confiabilidade. Para isso foi feita uma possível solução na ferramenta Cisco Packet Tracer, onde retratamos uma rede de alta segurança e que serve de exemplo para departamentos governamentais ou até mesmo empresas que precisam de alta confiabilidade conforme mostrado na imagem abaixo.

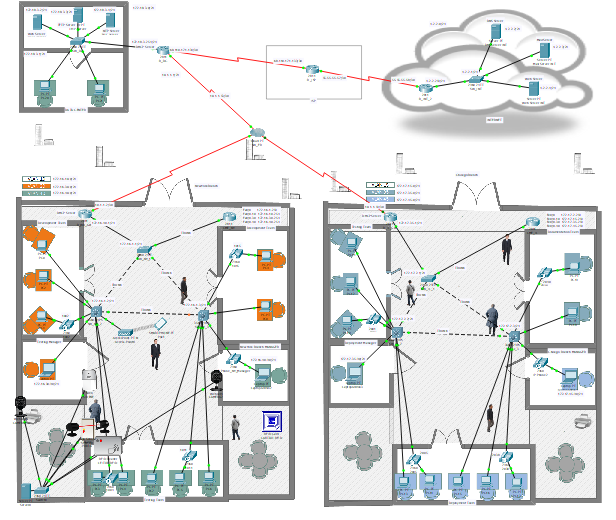


Figura 1- Projeto feito pelo grupo Hacktivismo na faculdade Fatec em junho de 2019.

No ambiente que criamos todos esses locais, exceto a sala do servidor local, estão conectados por meio de um switch de retransmissão de quadros para filtragem dos dados. O Data Center está conectado ao ISP para obter a Internet simulada (é uma rede 4.2.2.0/24). Algumas medidas com essas e outras precisam ser levadas em consideração para uma rede interna segura. Para uma boa solução, a empresa precisa contratar serviços de alta confiabilidade que existem no mercado empresas dedicadas a segurança da informação nas empresas. Mas para uma possível falha humana de segurança no local, ou seja, alguém sem permissão acessando uma área restrita, fizemos uma solução na sala do servidor, no projeto criado no Cisco.

Na solução proposta por nós, a sala do servidor que no exemplo é uma área de alta segurança, ou seja, pessoas não autorizadas não podem entrar. Para isso fizemos a seguinte limitações para o acesso a sala: para entrar na sala é preciso ter o RFID, que é tipo um cartão com permissão de acesso, que ao se aproximar da porta o sensor do RFID localizado próximo libera a porta para ser aberta. Quando a pessoa autorizada passa pela porta, um sensor de laser aciona duas câmeras localizadas uma dentro da sala e outra do lado de fora que tiram fotos simultaneamente da pessoa entrando e saindo da sala, além de que o sensor a laser também aciona uma sirene alertando que alguém está entrando ou saindo da sala.

**CONSIDERAÇÕES FINAIS**

O levantamento de dados realizado nesse trabalho foi com o intuito de mostrar as pessoas um método mais simplificado de ver e entender os ataques realizados por hacker de todos os estados do país.

Existem diversas vítimas, principalmente famosos e políticos, mostrando assim que os hacktivistas gostam de atacar quem tem algum poder ou está constantemente em mídia. Nenhuma pessoa está completamente segura e todos são possíveis alvos.

Alguns veem os hacktivistas como heróis, outros como vilões, mas uma certeza nós temos, eles crescem a cada dia mais e cada vez mais são reconhecidos pelo mundo.

Para desenvolver uma rede segura é preciso sempre pensar nas seguintes necessidades:

1. Acesso - Os usuários autorizados são fornecidos os meios para se comunicar de e para uma rede particular.

2. Confidencialidade - As informações na rede permanecem privadas.

3. Autenticação - Assegure-se de que os usuários da rede são quem eles dizem que são.

4. Integridade - Verifique se a mensagem não foi modificada em trânsito.

5. Não-repúdio - Assegure-se de que o usuário não refute que ele usou a rede.

(RAIHAN, Md. Asif, 2016)

**REFERÊNCIAS**

# ROHR, Altieres. [Como hackers tiram sites e serviços do ar: G1 Explica](http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-hackers-tiram-sites-e-servicos-do-ar-g1-explica.html). Brasil, 2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-hackers-tiram-sites-e-servicos-do-ar-g1-explica.html> Acesso em: 11 junho 19.

RAIHAN, Md. Asif; AFROZE, Marzia. **Securing a network by using vlan, port security and access control list.** EUA,2016.Disponível em: <http://dspace.ewubd.edu/bitstream/handle/123456789/2187/Md.\_Asif\_Raihan.pdf?sequence=1&isAllowed=y> Acesso em: 28 maio 2019.

# [DHAREDDY](https://www.youtube.com/channel/UCjLoPI87whBDSBvmjgBLh6w), [Srinivas](https://www.youtube.com/channel/UCjLoPI87whBDSBvmjgBLh6w). Enterprise network design in cisco packet tracer (6.1.1). Índia, 2014. Disponível em: <https://www.youtube.com/watch?v=3dhs9cl6M5E> Acesso em: 28 maio 2019.

LUGO, Guillermo. **Cisco packet tracer - configuración de rfid y trip sensor (iot).** Venezuela, 2018. Disponível em: <https://www.youtube.com/watch?v=6bqXmkjTRa4> Acesso em: 4 junho 2019.